EXECUTION VERSION

AMENDMENT NO. 1

TO

MASTER SERVICES AGREEMENT

This Amendment No. 1 ("Amendment No. 1"), effective as of February 28, 2013 (the "Amendment No. 1 Effective Date"), is made to that certain Master Services Agreement (the "Original Agreement") first dated as of December 13, 2012 (the "Original Agreement Effective Date") by and between State of Vermont ("SOV") and CGI Technologies and Solutions Inc. ("Supplier", and together with SOV the "Parties"). Unless otherwise defined herein, capitalized terms used herein shall have the meanings given to such terms in the Original Agreement.

WHEREAS, in connection with execution of the Original Agreement, the Parties agreed to negotiate in good faith during the period from the Original Agreement Effective Date to the Revised Scope Date (as defined in Statement of Work No. 1 between the Parties) to agree on certain matters, including the terms of Exhibits C, D, E, and L (the "Revised Scope Date Matters"); and

WHEREAS, the Parties wish to amend the Original Agreement to reflect their agreement on certain of the Revised Scope Date Matters; and

WHEREAS, the Parties wish to continue their good faith negotiations, to be concluded no later than the Revised Hosting Scope Date (as defined in the Amended and Restated Statement of Work No. 1 between the Parties), in order to finalize the scope of the hosting services.

NOW, THEREFORE, in consideration of the promises herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and intending to be legally bound hereby, the Parties agree as follows:

1. That the following shall be added as a new Section 15.9 of the Original Agreement:

> **15.9 <u>Supplier Rights to Use Work Product</u>.** Notwithstanding anything herein to the contrary, SOV hereby grants Supplier, subject to any restrictions applicable to any Third-Party Software embodied in the Work Product and excluding Customer Data, a perpetual, nontransferable, non-exclusive, royalty-free, paid-up right and license to use, copy, modify and prepare derivative works of the Work Product (excluding Customer Data) for the sole and limited purpose of providing IT Services to another State in furtherance of such State's development and operation of a State health insurance exchange pursuant to the Patient Protection and Affordable care Act of 2010. Supplier will provide written notice to SOV of any such use. With respect to Work Product that relates to Armedica, Inc.'s Onegate proprietary software product performed by Exeter Consulting ("Exeter Work Product"), SOV hereby grants Supplier, subject to any restrictions applicable to any Third-Party Software embodied in the Exeter Work Product and excluding Customer Data, a perpetual, irrevocable, non-exclusive, royalty-free, paid-up right and license, transferable to any successor to Exeter Group's business, with the right to sublicense, to use, copy, modify and prepare derivative works of the Exeter Work Product (excluding Customer Data) for any business purpose, except that during the period from the date hereof ending December 31, 2014, Supplier will not, and will ensure that during such period Exeter Consulting will not, directly or indirectly, license the Exeter Work Product for, or use the Exeter Work Product in any respect for the provision of services for, a

health insurance exchange solely devoted to the State of Vermont other than the Exchange (as defined in Section 1.2).

2. Exhibit C to the Original Agreement is hereby deleted in its entirety and replaced with the Exhibit C attached hereto as Attachment 1.

3. Exhibit D to the Original Agreement is hereby deleted in its entirety and replaced with the Exhibit D attached hereto as Attachment 2.

4. Exhibit E to the Original Agreement is hereby deleted in its entirety and replaced with the Exhibit E attached hereto as Attachment 3.

5. Exhibit L to the Original Agreement is hereby deleted in its entirety and replaced with the Exhibit L attached hereto as Attachment 4.

6. That, notwithstanding anything to the contrary herein, in the Amended and Restated Statement of Work No. 1, or any other agreement between the Parties, the Parties will negotiate in good faith during the period up to and including the Revised Hosting Scope Date to agree to the scope of the hosting services. The Parties further agree that, Exhibit D, Exhibit I, Exhibit L and, as necessary, other related documents will be revised to reflect the mutually agreed terms by the Revised Hosting Scope Date.

Except as modified by this Amendment No. 1, all provisions of the Original Agreement remain in full force and effect.

[*signature page follows*]

IN WITNESS WHEREOF the Parties have executed this Amendment No.1 as of the Amendment No. 1 Effective Date.

STATE OF VERMONT

By: E-SIGNed by Mark Larson on 2013-Mar-01

Name: _____

Type or Print

Title: _____

CGI TECHNOLOGIES AND SOLUTIONS, INC.

By: E-SIGNed by Gregg Mossburg on 2013-Mar-01

Name: _____

Type or Print

Title: _____

ATTACHMENT 1
Exhibit C

[see attached]

Exhibit C - Critical Milestones

1. **Liquidated Damages.** Each party agrees that the failure by Supplier to meet each Critical Milestone (as defined below) will cause SOV to suffer substantial damages which are difficult to estimate. Each party represents after all diligence it has determined appropriate, that the liquidated damages set forth below ("**Liquidated Damages**") are reasonable estimates of the damages which SOV will suffer for a failure to meet each Milestone set forth below ("**Critical Milestones**"), and agrees that the Liquidated Damages are not a penalty. Each party agrees that the Liquidated Damages are intended to be reasonable estimates of the actual damages that SOV would suffer, and are enforceable, valid and binding upon it. In the event that SOV elects to seek actual damages consistent with the terms of the MSA for Supplier's failure to meet one or more Critical Milestones, any Liquidated Damages paid in connection with such Critical Milestones shall be deducted from any damages award. If any Liquidated Damages are held to be unenforceable, then such Liquidated Damages shall be deemed deleted from this Exhibit C, and SOV shall have the right to recover such damages as it is able to recover under the MSA.

2. **Go-Live.** For clarity and without limitation, the failure to meet the Go-Live date of October 1, 2013 is not subject to Liquidated Damages, and SOV shall have the right to recover such damages as it is able to recover consistent with the terms of the MSA for any such failure.

3. **Excused Delay.** Notwithstanding anything to the contrary herein, Supplier shall not be liable for Liquidated Damages under this Exhibit C to the extent that the failure to meet any Critical Milestone is attributable in any material respect to the failure of SOV or SOV Third Party Resources to perform their obligations as set forth in the MSA (including this Statement of Work) or that arise out of causes beyond the reasonable control and without any material error, negligence or breach of Supplier obligations under the MSA (including this Statement of Work) of Supplier or Supplier Third Party Resources, provided that:

   a. Supplier provides written notice of the delay or failure promptly after first learning of the same describing the cause of such delay or failure in reasonable detail and includes it on all subsequent red-yellow-green reports until it is resolved, and escalates the matter to the SOV Deputy Commissioner of the Exchange within the Department of Vermont Health Access if any such delay is not redressed within two (2) weeks of such written notice from Supplier; and

   b. Supplier takes all reasonable efforts to avoid and minimize the impact of such failure by SOV or SOV Third Party Resources or such causes.

4. **Cap on Liquidated Damages.** In no event shall Supplier's total aggregate liability for all Liquidated Damages assessed under this Exhibit C exceed 10% of the total Detailed Deliverables Cost (as defined in Exhibit L (Pricing) (the "Liquidated Damages Cap"). The parties acknowledge and agree that the Liquidated Damages Cap will increase or decrease consistent with any increase or decrease in the total Detailed Deliverables Cost.

5. **Final Critical Milestones.** The date by which each Critical Milestone must be met is detailed in the chart below:

CMS Reference Number	Critical Milestone	HBE Project Date	Liquidated Damages
2.4	Call center live (CRM)	9/1/2013	High
2.5	Website launched	9/1/2013	High
9.2	Functionality demonstrated for PM Exchange Components (e.g. QHP Evaluation and Certification, Issuer Portal)	04/5/2013	Medium
9.2	Functionality demonstrated for E&E Exchange Components (e.g. enrollment processing, verification interfaces, rate calculator)	04/5/2013	Medium
9.2	Functionality demonstrated for FM Exchange Components (APTC/CSR data reporting, SHOP and individual premium billing)	04/5/2013	Medium
9.2	Functionality demonstrated for systems supporting Consumer Assistance functions (e.g. CRM, portal access)	04/5/2013	Medium
9.2	Development of PM Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013	High
9.2	Development of FM Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013	High
9.2	Development of E&E Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013	High
9.2	Development of CA Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013	High
9.2	Systems Testing complete and results submitted to CMS for all Exchange components	07/22/2013	Medium
9.2	Connectivity established for all required Data Services Hub services	06/3/2013	High
9.2	Hub and partner testing on all Data Services Hub services completed	06/3/2013	Low
9.2	Communications and security certification testing of all Data Services Hub services completed	06/25/2013	Medium

CMS Reference Number	Critical Milestone	HBE Project Date	Liquidated Damages
9.2	Preproduction testing of all Data Services Hub services completed	8/15/2013	Medium
9.2	Production environment setup completed	08/15/2013	Low
9.2	End-to-end testing completed	09/1/2013	High
9.2	State test summaries and results of CMS-developed test scenarios submitted to CMS	09/1/2013	Low
10.3	Substantially completed Safeguard Procedures Report submitted to IRS for approval	06/25/2013	Medium

6. **Amount of Liquidated Damages.** The parties agree that the amount of damage to SOV will be as follows:

For Critical Milestones categorized as Low:

- $3,750 for every day late from 1 to 3 days late per Critical Milestone;
- $7,500 for every day late from 4 to 7 days late per Critical Milestone;
- $10,000 for every date late from 8 to 14 days late per Critical Milestone;
- $25,000 for every day late after 14 days late per Critical Milestone.

For Critical Milestones categorized as Medium:

- $9,375 for every day late from 1 to 3 days late per Critical Milestone;
- $18,750 for every day late from 4 to 7 days late per Critical Milestone;
- $25,000 for every day late from 8 to 14 days late per Critical Milestone;
- $62,500 for every day late after 14 days late per Critical Milestone.

For Critical Milestones categorized as High:

- $18,750 for every day late from 1 to 3 days late per Critical Milestone;
- $37,500 for every day late from 4 to 7 days late per Critical Milestone;
- $50,000 for every day late from 8 to 14 days late per Critical Milestone;
- $125,000 for every day late after 14 days late per Critical Milestone.

As provided for in Section 5, the total Liquidated Damages assessed under this Exhibit C shall not exceed the Liquidated Damages Cap.

7. **Payment.** Supplier shall pay any Liquidated Damages due to SOV hereunder within 30 days of the date on which the applicable Critical Milestone was originally due to be met, or, at SOV's option, such amounts may be deducted from all or any portion of the Charges payable to Supplier in accordance with the MSA. SOV shall notify Supplier in writing before SOV deducts such sums from the Charges.

8. **Earnback.** If Supplier meets all criteria set forth below for the Go Live Launch of the Exchange by October 1, 2013, then Supplier will be entitled to earn back fifty percent (50%) of the Liquidated Damages paid to SOV under this Exhibit C. The Supplier's earn back of Liquidated Damages is not a waiver by SOV of any right it may have under the Agreement.

9. **Modification or Waiver.** Any Liquidated Damages payable under this Exhibit C, including the Critical Milestones, dates for completion and amounts of Liquidated Damages, may be changed at any time by written agreement of the parties, but only by means of a Change Order. The parties further agree that the applicability of the Liquidated Damages to the performance of a Critical Milestone may be waived by SOV in any given instance, but only pursuant to a written waiver signed by the Commissioner of Vermont Health Access.

10. **Acceptance Criteria**. The final acceptance criteria shall be as agreed upon by the parties and set forth in the PMP.

8617v.6

ATTACHMENT 2
Exhibit D

[see attached]

Exhibit D

Service Levels

1. Hosting Services Service Levels

a. Generally. The Health Benefits Exchange applications and associated hosting (together, the "System") have been designed and will be implemented and operated to run in compliance with the Service Levels set forth in this Section.

b. Summary Table. The following Service Levels and Service Level Credits apply to the Hosting Services (as defined in Exhibit I to the MSA), subject to the provisions that follow in Section 1.c below.

Service Level Agreement (SLA)	**Service Level**	**Service Credit for Failure**
Availability During All Hours	For each hour:	
	Production: 99.90% Egregious: 94% Non-Production: 99.5%	$3,500 Egregious: $5,000
Content Maintenance	Timely Updating of Production Content Per Agreed Schedule	$1,500 for each Scheduled Update
Web Page Response Time	Production: 1 second average	For each day: $1,000
	Egregious: 5 second average in any hour 3 times in any day or 10 times in a week	Egregious: $5,000 each day or week
Response Time for Real Time Transactions	Production: 90% within 5 seconds None greater than 10 seconds	For each day: $1,000
	Egregious: 75% within 5 seconds None greater than 10 seconds	Egregious: For each day: $5,000
Help Desk Mean Time to Restore Severity Level 1	4 Hours	$5,000 per day
Where "Restore" means that CGI has done one of the following: 1. Correct the problem; Provide workaround; or 2. Correct a portion of the problem to reduce the	Egregious: Any greater than 24 Hours	$500 per hour

Severity Level		
Help Desk Mean Time to Restore Severity Level 2	8 Hours	$5,000 per day
Where "Restore" means that CGI has done one of the following: 1. Correct the problem; 2. Provide workaround; or 3. Correct a portion of the problem to reduce the Severity Level	Egregious: Any greater than 5 days	Egregious: $500 per hour
Help Desk Mean Time to Resolve Severity Level 1 Where "Resolve" means that CGI has fixed the root cause and removed the workaround	According to agreed plan identified and agreed as part of problem restore activities. Daily update on status.	
Help Desk Mean Time to Resolve Severity Level 2 Where "Resolve" means that CGI has fixed the root cause and removed any workaround	According to agreed plan identified and agreed as part of problem restore activities. Daily update on status.	

Note: "**Workaround**" means a temporary fix that is reasonably acceptable to SOV and that does not resolve the underlying problem, but provides the proper results required of the System (through manual processing or otherwise).

Backup and Recovery	All daily and weekly backups executed successfully 1 hour recovery start, 4 hour completion	$500 Each missed daily Backup $2,500 Each missed weekly Backup $500 Each late Recovery $2,500 Each failed Recovery
	Egregious: Failure of any 3 consecutive backups or recoveries	Egregious: $15,000
Batch Completion	Completion of critical time sensitive batch processes complete within agreed timeframes to be collectively defined and agreed during design phase.	$2,500 each violation
	Egregious: TBD Completion	Egregious: $5,000
Disaster Recovery	4 Hour RTO, 30 Minute RPO	$100,000 each violation

c. Service Level Descriptions.

i. Availability During All Hours

1. Definitions.

a. "**Availability**" means the availability for use by intended individual users, System processes or interfacing systems of all features, functions and processes of the System.

b. "**All Hours**" means: All time 7 x 24 each week.

c. "Minor Maintenance Window" means the second and fourth weekend of each calendar month starting at 2:00 a.m. EST Saturday and continuing until 5 a.m. EST Sunday, provided, however that SOV may require a different maintenance window timeframe as SOV determines is necessary, in SOV's reasonable discretion. **System Availability will be unaffected during Minor Maintenance Windows**

d. "Major Maintenance Window" means twice a year on dates and times agreed to by SOV and CGI, during which CGI will be allowed to schedule a maximum of 8 hours of larger System modifications and maintenance.

e. "Scheduled Maintenance" means System maintenance described in written notice from CGI at least five (5) days in advance that may require unAvailability that is performed within the Minor or Major Maintenance Windows and in accordance with such notice from CGI, and for which CGI timely posts a notice of Scheduled Maintenance on the Website according to agreed procedures.

f. **"Scheduled Maintenance Downtime"** means any period of unAvailability for Scheduled Maintenance.

2. Measurement. The System will be configured to alarm the unAvailability of any key aspect of the System, and in addition, any unAvailability reported through the Help Desk will be included in the calculations of Availability from the time the unAvailability was first known by CGI either through alarms, the knowledge of its personnel or a report by SOV or another user. CGI will use reasonable efforts during the Statement of Work Term to expand the monitoring capabilities of the System to automatically detect unAvailability of any aspect reported hereunder but not detected by the System automatically. This Service Level will be determined by dividing the number of hours of Availability in the month by the total hours in the month. However, Major Maintenance Window Scheduled Maintenance Downtime will not be included in the calculations for the numerator or the denominator to determine performance on this Service Level

3. Service Level Credit. The Service Level Credit will be determined by taking the difference between the required number of hours of Availability in the month and the actual number of hours of Availability during the month, and if a positive number, multiplying the difference (if any) (rounded to the next highest full hour) by the Service Level Credit amount set forth in the Summary Table.

ii. Content Maintenance

1. Definitions.

a. "Content" means all information and materials to be posted on the Website.

2. Description of Service Level. The parties will establish an update schedule for updating the Content on the Website. The Service Level measures compliance with each update required under that schedule (each is a "**Scheduled Update**").

3. Measurement. Each Scheduled Update is required to be completed no later than the date and time scheduled, with all Content set for that Scheduled Update successfully updated on the Website.

4. Service Level Credit. The Service Level Credit in the Summary Table above will be multiplied by the number of Scheduled Updates not completed on time during the month.

iii. Web Page Response Time

1. Definitions.

a. "Web Page" means an individual document created in HTML that is displayed when a user visits the web page's uniform resource locator address.

b. Description of Service Level. This Service Level measures daily average time that the Web Pages comprising the Website take to respond to a request sent by a user through the user's browser.

c. Measurement. Each day, through an agreed automated process, CGI will sample Web Page responses on no less frequently than every five (5) minutes and compile hourly and daily statistics for specific Web Pages designated by SOV and an aggregate average response time.

d. Service Level Credit. The Service Level Credit in the Summary Table above will be multiplied by each day that the average is above the Service Level. The Egregious Service Level Credit will be paid for each time that the Egregious Service Level is exceeded for the hourly averages in a day or in a week, as applicable, measured for this Service Level.

iv. Response Time for Real Time Transactions

1. Definitions.

a. "Real Time Transaction" means a transaction between a user of the Website and the Exchange where data is sent from the user after logging in to the user's account and requires processing by the Exchange and a response to the user.

2. Description of Service Level. This Service Level measures daily average time that the Web Pages comprising the Website take to respond to a request sent by a user through the user's browser.

3. Measurement. Each day, through an agreed automated process, CGI will sample Real Time Transactions on no less frequently than every five (5) minutes and compile daily statistics for specific Real Time Transactions designated by SOV and an aggregate average response time.

4. Service Level Credit. The Service Level Credit in the Summary Table above will be multiplied by each day that the average is above the Service Level. The Egregious Service Level Credit will be multiplied by each day that the average is above the Egregious Service Level.

v. Help Desk Mean Time to Resolve Severity Level 1

1. Description of Service Level. This Service Level measures the mean time for CGI to resolve Severity Level 1 incidents from the time first reported to CGI.

2. Measurement. CGI's trouble ticketing system will automatically track the time from initiation of the incident to closure. The incident will be initiated immediately upon notice to CGI.

3. Service Level Credit. The Service Level Credit in the Summary Table above will be multiplied by each day that the average is above the Service Level. The Egregious Service Level Credit will be multiplied by each hour that is above the Service Level.

vi. Help Desk Mean Time to Resolve Severity Level 2

1. Description of Service Level. This Service Level measures the mean time for CGI to resolve Severity Level 2 incidents from the time first reported to CGI.

2. Measurement. CGI's trouble ticketing system will automatically track the time from initiation of the incident to closure. The incident will be initiated immediately upon notice to CGI.

3. Service Level Credit. The Service Level Credit in the Summary Table above will be multiplied by each day that the average is above the Service Level. The Egregious Service Level Credit will be multiplied by each hour that is above the Service Level.

vii. Backup and Recovery

1. Definitions.

a. "Backup" means a copy of the data stored in the System used for Recovery purposes.

b. "Recovery" means the loading of data from a Backup into the appropriate database of the System.

2. Description of Service Level. This Service Level measures completion of the scheduled Backups and of all necessary Recoveries each month.

3. Measurement. All Backups and Recoveries will be monitored by the System and completion and failure automatically reported. Time for each Recovery will be measured by the System from start to completion and reported automatically.

4. Service Level Credit. The Service Level Credit in the Summary Table above will be multiplied by failure to complete the Backup each day that the average is above the Service Level. The Egregious Service Level Credit will be paid for each time that the Egregious Service Level is exceeded.

viii. Batch Completion

1. Definitions.

a. "Batch" means a scheduled program that runs without user intervention. CGI will maintain a list of all Batch jobs run by the System.

2. Description of Service Level. This Service Level measures completion of scheduled Batch jobs.

3. Measurement. All Batch jobs will be monitored by the System and completion and failure automatically reported.

4. Service Level Credit. The total number of Batch jobs completed each day will be divided by the total Batch jobs for the day, and if that quotient is less than the Service

Level, Service Level Credit will be paid for that day. The Egregious Service Level Credit will be paid for each time that the Egregious Service Level is exceeded.

5. Reserved.

ix. Disaster Recovery

1. Definitions.

a. "Disaster" means a Force Majeure Event or other circumstance causing any part of the System to be unAvailable and requiring that any portion of the System be moved to another data center to restore full Availability.

b. "RPO" means the Recovery Point Objective, the maximum period for lost data in the event of a Disaster.

c. "RTO" means the Recovery Time Objective, the maximum time to recovery all System Availability at another data center after a Disaster.

2. Description of Service Level. In the event of a Disaster, CGI will meet the RPO and RTO to recover the System and restore full Availability.

3. Measurement. The Service Level will be measured from the declaration of a Disaster pursuant to agreed procedures until full System Availability has been restored.

4. Service Level Credit. The Service Level Credit will be paid for each failure to meet the RPO or the RTO.

x. Cap on Service Level Credits. In no event shall the total Service Level Credits for the Hosting Services exceed twenty percent (20%) of the total amount billed each month for such Services. Provided, that if any amount of Service Level Credits is excluded as a result of this cap, any Earn Back Credits will be reduced by the amount of such exclusion.

2. Commencement. The Hosting Services Service Levels apply beginning on Go-Live.

3. Exclusions. CGI's failure to meet any Service Level will be excused, and not counted in the calculation of any Service Level (in a manner that excludes the failure in every respect so that CGI is neither better nor worse off in Service Level calculations because of such failure) to the extent that CGI's failure is caused by one of the following circumstances, so long as CGI uses reasonable efforts to avoid and minimize such failure as applicable and consistent with its obligations under this MSA ("**Exclusions**"): (i) acts, errors and omissions of SOV or any of SOV's suppliers or contractors including but not limited to any breach, failure or delay by SOV, SOV's suppliers or contractors to timely and effectively satisfy their responsibilities under this MSA (or agreements with SOV related to the same) and to provide timely decisions and approvals as required under this MSA; (ii) a Force Majeure Event (subject to compliance by CGI with its obligations arising under this MSA in connection with such Force Majeure Event); (iii) any circumstance where CGI is prohibited by applicable Law from taking actions required to correct such failure so long as CGI has provided prompt notice to SOV of the basis and extent of such prohibition and has proposed appropriate efforts to address the same for approval by SOV; (iv) service or resource reductions requested or approved by SOV and agreed to by the parties through the Change Control Procedures; or (v) if any of the assumptions set forth in this Statement of work are exceeded and through the Change Control Procedures the Parties identify additional hardware, software, or telecommunications resources required to meet SOV's needs the costs for which are additional Charges under this Statement of Work, and for which SOV does not agree to such change and does not approve the addition of such resources (and payment of such additional Charges). For clarity, adverse performance of the components of

the System is not a Force Majeure Event. If the same incident causes multiple Service Levels to be missed, CGI shall only pay to SOV the highest applicable Service Level Credit associated with the root cause generating such missed Service Level (as opposed to a Service Level Credit for each single missed Service Level).

4. Service Level Credits

a. Calculation. Service Level Credits will be calculated as set forth in each Summary Table and the other provisions of this Exhibit D. Service Level Credits will be determined each calendar month during which Service Levels apply.

b. Earn-Back. If in any month CGI pays Service Level Credits for any failure to meet any Hosting Service Levels (but not any month in which it pays any Egregious Violation Service Level Credits) (such Service Level Credits are the "**Earn Back Credits**"), and for the next three (3) months CGI does not owe any Service Level Credits, then CGI will be credited with the Earn Back Credits to offset against any future Service Level Credits for that category (but not Egregious Service Level Credits). For clarity, the Earn Back Credits will not be paid in cash, and if this Statement of Work terminates with CGI having a balance in Earn Back Credits, such Earn Back Credits will expire and have no force or effect.

c. Payment. Service Level Credits accruing in one month will be automatically offset against the following month's invoice.

5. SLA Reports. CGI will provide the following SLA reports for each calendar month no later than the 15th day of the following calendar month:

a. Compliance. CGI will provide a monthly SLA compliance report described in a form acceptable to SOV. Each monthly SLA compliance report will report on SLA compliance in both raw form (without taking into account any Exclusions) and then adjusted (taking into account any Exclusions), each of which will be clearly explained in reasonable detail in the monthly SLA compliance report.

b. Incidents. CGI will provide a monthly report summarizing the incidents reported during the month by Severity Level, and their resolution, and root cause determinations for each.

c. Trending. CGI will provide monthly, quarterly and annual SLA trending reports requested by SOV.

d. Analysis and Recommendations. At least every six (6) months, CGI will provide a brief analysis of its SLA performance and recommendations for improvement of its performance.

e. Special. CGI will provide such other information regarding SLAs, performance of the System and Services and other metrics as SOV may request from time to time.

6. Raw Data. CGI will make available to SOV an electronic version of all raw data used to create the SLA report each month

7. Termination. Pursuant to Section 26.2(c) of the MSA, SOV's right to terminate thereunder includes the following:

a. Repeat SLA Violations. SOV will have such right if CGI fails any of the same SLA for three (3) consecutive months or any four (4) months in any twelve (12) month period or if CGI fails at least three (3) SLAs in each of three (3) consecutive months or any four (4) months in any twelve (12) month period.

b. Egregious SLA Violations. SOV will have such right in the event of any Egregious violation. The definition of Egregious violations herein is not intended to set the bounds of a

material breach of the MSA, and the parties agree that such definitions will not be used to limit the scope of the definition of a material breach of this Agreement. Each Egregious violation sets forth a Service Level Credit, and for each violation, SOV may elect to terminate under this Section, or receive that Service Level Credit, but not both.

c. Timing of Termination. If SOV elects to exercise the termination rights stated in this Section 9, SOV must elect such right within twenty (20) business days of SOV's delivery of written notice to CGI of the applicable violation.

ATTACHMENT 3
Exhibit E

[see attached]

EXHIBIT E – SCOPE ASSUMPTIONS

The following assumptions are intended to augment the RTM and assist the SOV in understanding the basis Supplier has developed with regard to defining the Project scope, timing, resources, roles and responsibilities, and cost. Any required changes to these assumptions will be addressed by the Parties through the Change Control Procedures.

These Scope Assumptions are part of the Master Services Agreement (MSA).

1.1.1. General Project Assumptions

The project under SOW No. 1 (the "Project") began on December 17, 2012. The project team will be co-located in the Williston area at a location to be provided by the SOV.

- Elaboration Assumptions.
  - Prototypes will be demonstrated to selected super users on an ad hoc scheduling basis.
  - Iterative development will include functionality that can be built during the allotted timeframe as defined in the WBS, defined as deliverable D-01 (Baseline Schedule – WBS).
  - Subsequent iterations will include further refinements to previous iteration functionality as time allows as defined in the Project Work Plan.
  - All prototype workshops will take place at a single location and make use of web conferencing to provide access to users who cannot attend workshops directly.

During testing (of all testing types), defects will be classified by the SOV and Supplier collaborating in good faith. If the Parties disagree as to a classification, then SOV's classification will govern. Defects will be classified as follows:

Level	Category	Description
1	Sev1	**Essential Business Process Affected** - Any highly critical system or service outage that results in loss or severe degradation of material business processes and/or capabilities, including those that are defined as "must have" in the finalized requirements, and for which there is no acceptable workaround, as determined by SOV in its reasonable discretion. (Availability of workaround renders it "Sev2")
2	Sev2	**Part of an Essential Business Process or Workgroup Affected** - Degradation of system or service performance that impacts end user service quality or significantly impairs business process control or operational effectiveness for material functionality, including functionality defined as "must have" in the finalized requirements, but for which there is an acceptable workaround.
3	Sev3	**Non-Essential Business Process or Workgroup or Individual Affected** - Minor degradation of system or service performance that does not have any impact on end user service quality. These are typically cosmetic defects.
4	Doc	**Documentation Defect** Error or omission in document.

- The SOV and Supplier will coordinate to establish a series of regular, formal reviews of the project progress, issues, and strategies for risk mitigation.

- Supplier's Proposal to the SOV outlines Supplier's tasks and obligations for the HBE implementation project. In addition, Supplier has provided an organizational chart of expected staffing in Section 1.1.3.2 of this Exhibit.
- At the SOV's request to provide more granularity and transparency on project spend, Supplier will track and report the monies earned based on the services provided and deliverables furnished as set forth in Exhibit L. Specifically, these reporting requirements and supporting payment processes will be further described in the mutually executed PMP and agreed-upon payment processes. Supplier will establish the SOV Project Library using its CPMF standard Ensemble SharePoint project repository. This Project Library provides mutual access to all project artifacts, including but not limited to deliverables, and tracking tools for risk and issue management. During project startup, Supplier and the SOV will mutually determine read and update access for the Project Library as well as the process for transferring completed deliverables to the SOV Document Library.
- To the extent that Supplier has entered into other contracts with any other States, Exchanges, or the Federal Government relating to the design, development or operation of an Exchange system, Supplier as part of the project plan shall proactively identify, review, discuss and submit recommendations to the SOV regarding reuse of work from these other contracts. In determining how to reuse available design and development components and best to serve the interests of SOV, Supplier will evaluate all options from both a cost and timeline perspective in making a recommendation.

1.1.2. Project Work Plan Assumptions

- The SOV HBE Project Manager is responsible for reviewing available options and Project issues in a timely manner (i.e., within five (5) business days, or as mutually agreed to by the SOV HBE Project Manager and Supplier Project Manager) in order to minimize delays to the Project schedule. If resolution cannot be made within the five (5) business days (or as mutually agreed to by the SOV HBE Project Manager and Supplier's Project Manager), the SOV HBE Project Manager will raise the issue to the Deputy Commissioner and/or Commissioner within two (2) additional days.
- The Commissioner, members of the Executive Committee and Supplier Executives will form an Advisory Board to resolve issues affecting or involving other organizations and stakeholders that the Project Management Team has identified and cannot resolve in a timely manner. The Advisory Board will make decisions within 2 business days form the request for resolution of an issue.
- The below preliminary criteria must be met for Go-Live. The SOV and Supplier will develop final Go Live criteria as set forth in the PMP and conduct Preliminary Operational Readiness and Operational Readiness Reviews to assess the Exchange and supporting infrastructure and staff for readiness to Go Live. The Go-Live definition may be supplemented with criteria from the Operational Readiness Plan and/or Implementation Plan upon their completion.

Go-Live criteria:

- Tested code has been successfully released into the production environment
- SOV has reviewed and approved evidence of testing deliverables
  - **Network**: devices, connectivity, security
  - **Hardware**: Hosting environment, servers, universal power supply (UPS), storage, backup server(s) in place
  - **Interfaces**: All in scope Federal and State system interfaces and interfaces with key partners (e.g., Carriers, Premium Processing vendor, Customer Support, etc.)
  - **Software**:
    - Unit testing to ensure all system build is complete for:
      - Screens
      - Templates
      - Reports
    - System testing to ensure data pass from one function to another to support critical workflows in each of the CMS identified Exchange Components per 7/22/2013 milestone in Exhibit C
  - Security, Performance, and Load testing is complete

- All deliverables have been approved by SOV and submitted to CMS
- Post-Production Readiness plan

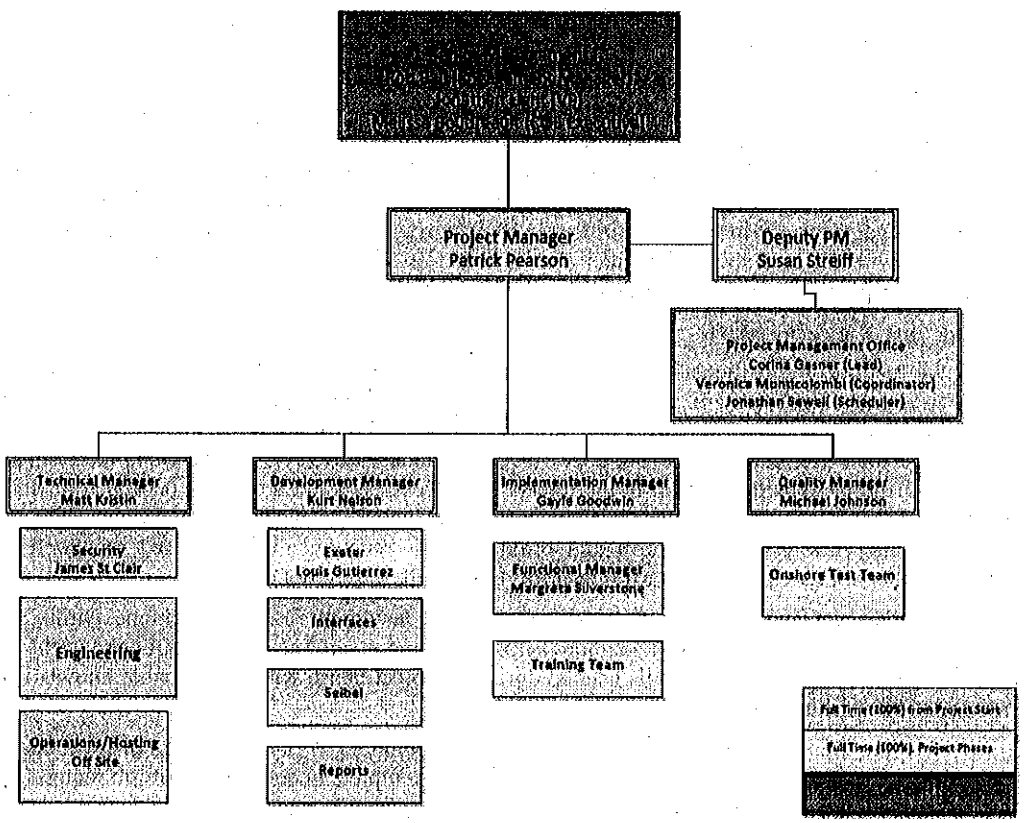
1.1.3. Staffing Assumptions

1.1.3.1. SOV

- The SOV is responsible for appointing a dedicated full-time SOV resource to establish and manage a project team to work on the Project and provide for timely completion of the SOV's Project responsibilities. Supplier has provided a list of roles expected to be provided by SOV in Section 1.3.
- The Department of Vermont Health Access, in conjunction with Department of Information and Innovation (DII) and Agency of Human Services (AHS)-IT, is responsible for facilitating the participation of other State agencies and insurance carrier staff as required to assist in the design, development and testing of State of Vermont agency interfaces and State insurance carrier interfaces.
- Supplier will incorporate SOV tasks and estimated level of effort to the project schedules through the lifecycle of the project. This view of SOV responsibility will be tracked through the regular project management approach facilitated by the SOW and Supplier project management.

1.1.3.2. Supplier

Supplier will have the following staffing in place for the Project:



Supplier's resource plan as of February 1, 2013 is as set forth below. The resource plan will be adjusted in alignment with the Project Work Plan, as required.

Staffing Table

Period	21-Jan	4-Feb	18-Feb	11-Mar	25-Mar	9-Apr	23-Apr	7-May	21-May	4-Jun	18-Jun	16-Jul	31-Aug	30-Sep	30-Oct	Nov-31	31-Dec
Staff Group																	
Senior Management	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
PMO	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Technical	2	4	6	10	12	12	12	12	16	16	16	16	16	16	16	12	8
Development	2	4	4	8	10	12	12	15	15	15	15	15	15	15	12	10	8
Implementation	2	4	6	10	12	12	12	12	16	16	16	16	16	16	16	14	8
Quality /Testing	2	4	4	6	8	10	10	10	10	10	10	10	10	10	10	8	8
Admin		1	1	2	2	2	3	3	3	3	3	3	3	3	3	3	3
Total	**16**	**25**	**29**	**44**	**52**	**56**	**57**	**60**	**68**	**68**	**68**	**68**	**68**	**68**	**65**	**55**	**43**

PROJECT STAFFING REQUIREMENTS

- Supplier, to successfully fulfill the delivery of the SOV's Exchange projects within the prescribed timeframes, shall address staffing requirements as needed. Supplier will/has assign a senior member of its HR team to be its company-wide HIX Staffing Coordinator. The Staffing Coordinator is exclusively focused on staffing the Project and will coordinate the staffing between Supplier's internal organizations (internal staffing, external recruitment) as well as selected contracted external recruitment. Within our contracted external recruitment, Supplier will engage two main types of firms: (1) third party recruiting firms who are focused on recruiting national talent with HIX, health and human services, and/or specialized technical skills and (2) third party recruiting firms who are focused on recruiting qualified local talent.

Identifying and Acquiring Staff

- Based on the position requisitions, Supplier shall identify potential candidates to fill each position through resume review and initial screening. This applies to both existing Supplier resources as well as external candidates sourced from either Supplier's external recruiting team or by third party contracted recruiting firms. Candidates are then presented to the Supplier's Project Manager to review. The Supplier Project Manager selects which candidates will move on in the interview process. Supplier's staffing organization shall conduct three interviews with at least one of the three interviews being an in-person interview. Each interviewer completes an interview assessment form and provides their recommendation. Based on the feedback, the candidate is either approached with an offer or informed that they were not selected.
- Existing staff that are completing their assignments are considered first for positions within the project, depending on the skills match. This method helps to support staff continuity throughout the life of the project. It is critical to balance the skills needed during a project phase with the valuable knowledge that staff members gain by working on the project.
- Whether recruiting internal staff or external job candidates, recruiters work closely with hiring managers throughout the recruitment process to make sure they have a complete understanding of job requirements, that candidates are sourced and referred to hiring managers that possess the requisite knowledge and skills for each position, and that positions are filled in accordance with the schedule, operational needs, as well as providing compliance with State employment-related regulations.

- Staffing processes include accountability, processes, and procedures to effectively and efficiently meet staffing requirements, State requirements, and Federal hiring practices. Supplier will ensure flexible and scalable enough to meet changing requirements and operational demands quickly and efficiently.
- Factors such as specific skill sets, experience of staff at commensurate projects, outcome successes of specific staff, cultural fit, and bench strength of the organizations supplying staff are all taken into consideration when determining how and where to acquire staff. For the Project, factors taken into consideration include:
  - Complexity and size of the project
  - Implementation of newer technologies
  - Types of business problems being addressed
  - Timeframe to implement
  - Proximity to project site and/or experience with virtual teaming
- **Change of Staff**

  Supplier will utilize the same hiring process outlined above in the event there may is a need to provide replacement or additional personnel. Replacement personnel may be required when planned staffing changes result from periods of increased project activity (those periods tracked and planned for in the Schedule across the SDLC). Additionally, when the project experiences an unplanned loss of staff, the Supplier's team is required to identify their replacement.

  Supplier is especially focused on mitigating the impact of unplanned loss of staff since the Exchange Schedule is aggressive. The Supplier's Project Manager has the authority to escalate the priority of the staffing of any position so that resources are focused on staffing the most critical positions first. At a corporate level, Supplier shall maintain a bench of project consultants (both functional and technical) that can be evaluated immediately if an unplanned loss of staff occurs. The Staffing Coordinator shall maintain a pipeline of external candidates particularly with HIX, health and human services and/or specialized technical expertise that can be tapped in the event of a sudden unplanned loss of staff on the Exchange Project. The Exchange Project team leads are directed to cross-train team staff as a stop-gap measure should an unplanned loss of staff occurs.
- **Key Staff**

  Certain roles on the project are defined as Key Staff as identified in the Organization Chart and Staffing Table located in Section 1.1.3.2 of this Exhibit. Positions that are designated as Key Staff will not remain vacant for more than 30 calendar days. Key Staff positions will not be filled with employees who are assigned to fulfill the roles and responsibilities of the position in a temporary capacity and/or maintain responsibilities for another position. Supplier shall report the replacement of Key Staff to the SOV IT Manager and HBE Project Manager and shall provide a resume for the replacement within three weeks of the Key Staff members' resignation, and will be subject to the SOV's written approval (not to be unreasonably withheld). Supplier roles and Project organization are set forth in the Organization Chart and Staffing Table above.

Supplier's Project Manager will coordinate its project activities with the SOV HBE Project Manager in regards to project-related items such as: financial reporting, contract amendments, invoicing, status reports, etc.

1.1.4. Facilities and Access

- The SOV is responsible for providing space and furnishings for Supplier to co-locate their project teams in a joint facility. Supplier is responsible for providing computer equipment needed for its staff.
- The SOV will provide badge access for Supplier personnel to identified locations for the duration of the Project as long as Supplier staff meet the SOV security requirements necessary to provide a badge.
- The SOV will provide wireless, internet connectivity to Supplier staff at the co-location site.

1.1.5. Deliverables & Standards Assumptions

- The SOV is responsible for reviewingPproject document deliverables in the timeframes specified in the PMP. The SOV and Supplier Project Managers may mutually agree to shorten or extend the review time should it be required. Any such change to the duration will be documented in the mutually agreed Project Schedule and/or

otherwise be documented in writing and agreed to by the SOV Project Manager and the Supplier's Project Manager.

- The review and approval of Change Orders will be performed using mutually agreed processes as defined in the MSA and Exhibit H.
- The resolution and documentation of issues will be performed using mutually agreed processes as defined in the PMP.
- Supplier will provide a deliverable transmittal / notification letter with each deliverable, including services-only deliverables using templates defined in the PMP.
- A list of the required deliverables to be completed by Supplier through are provided in this Exhibit E the Pricing Exhibit L.
- The Pricing Exhibit L and timeline for delivering Supplier services assume the timely and appropriate participation of the State of Vermont agencies in the updated Project Work Plan and as stated in the PMP. In the event timely participation is not secured, the Supplier Project Manager will work with the SOV Project Manager to escalate to the Deputy Commissioner or Commissioner for deliberation and resolution. A Change Order, utilizing the process identified in Exhibit H, may be executed upon mutual agreement if additional Supplier resources are warranted.

1.1.6. Hardware and Software Assumptions

- If it is mutually agreed that a third party software product is not needed to meet Exchange requirements, the software can be removed from the Exchange solution. This does not affect Supplier's obligation to meet all requirements of the Project.

1.2. Assumptions – Design, Development, Implementation (DDI)

1.2.1. Design and Requirements Validation

- Supplier will lead requirements verification sessions with the SOV, and provide updated requirements documents for review and sign-off by SOV Business Leads.
- Supplier will lead the Design sessions and use the One Gate System to facilitate a gap analysis between the existing system and what needs to be configured or developed for the SOV.
- The SOV will facilitate dedicated time from other agency functional and technical resources knowledgeable in their systems requirements to facilitate interface design.
- The following process will be followed in support of the Requirements Design Integration
  - Demonstrate and discuss the requirement
  - After the requirement is demonstrated, Supplier will ask SOV for agreement that the requirement has been met or validated. If the requirement is demonstrated in a way for which Supplier can validate that Supplier understands the requirement, but it is not met, the Supplier facilitator should indicate the requirement is being validated not met and we will be able to demonstrate at a later date, if needed.
  - There can be 4 basic results:
    - SOV agrees with no comment or action necessary (agreement is received that the requirement has been met, or validated in the case where Supplier is demonstrating the understanding of the functionality).
    - SOV agrees that Supplier has met the requirement but there is still an action item.
    - SOV agrees Supplier has met the requirement but with comments
    - SOV doesn't agree that Supplier has met the functionality. This should always have an action item for Supplier management, and possibly a comment. There should be a full description of why SOV doesn't believe the requirement has been met.
  - All action items and comments will be assigned a lead person and participants identified for resolution. The lead is responsible for getting the information or following up on the comment. A due date will also be assigned. The due date should be prior to the next scheduled meeting, if possible.

1.2.2. Development and Implementation

1.2.2.1. Solution Configuration Development and Testing

- Supplier will be responsible for Unit, Integration, System, and load testing with support from the SOV in reviewing and approving test cases and test results.
- Supplier will organize and support User Acceptance Testing (UAT). The SOV will provide resources to execute UAT scripts. Supplier and SOV will document a plan for development of the UAT scripts in the testing plan.
- The Establishment Review Process has replaced the Exchange Lifecycle as the current CMS guidance for Exchange deliverable review.
- Supplier will train SOV staff on the use and organization of Supplier Ensemble SharePoint project repository. The Supplier Ensemble SharePoint repository should be used to store only project management and delivery documentations; State-specific confidential data will not be stored in the Supplier Ensemble SharePoint repository.
- Supplier will work with the SOV to provide preliminary design review artifacts to support a "Design Consult" with CMS targeted for Q1 2013. Supplier will support the SOV-CMS design reviews by providing the artifacts defined as necessary by CMS for Federal Gate reviews.
- Exchange will support browsers consistent with CMS Guidance for web-based non-employee facing user interfaces. Exchange will support commonly used browsers (Internet Explorer 8 and above), Firefox (current and subsequent versions plus the two prior versions), Chrome (current and subsequent versions plus the two prior versions) and Safari (5.1 and subsequent versions).
- While a broad range of devices such as smart phones, tablets, and iPads that have modern web browsers that support HTML5 will be able to access the consumer portal, the full shopping, enrollment, and self-service capabilities of the Exchange require ample screen size (e.g., tablet and above) for appropriate usability.
- Any modifications to the existing eligibility legacy system (ACCESS) that may be required as a result of the implementation of MAGI eligibility will be accomplished outside the scope of this effort.

1.2.2.2. Interfaces

- The State and Federal Systems/Applications that integrate with the Exchange will be available during System Integration / UAT with data to test end to end scenarios.
- The SOV is responsible for facilitating Supplier's access to and ensuring the availability of access to SOV systems and interfaces.
- Supplier and the SOV have developed a list of required interfaces within the Project Work Plan, through the 'interface deliverables.' The SOV will provide such interfaces through inter-agency agreement with the State agencies and secure production files for the final testing of the system interfaces.
- Supplier will provide an interface to the Federal Data Services Hub, including:
    - Federal Exchange Eligibility Service Interface
    - CMS System Interface
    - Federal Hub Interface

- Other in-scope interfaces include:
  - Carrier System Interface
  - Other State Interfaces
  - Eligibility Systems Interface

1.2.2.3. Reporting

- The SOV will provide trained and qualified staff for reviewing and approving the reports requirements and designs developed by Supplier for the Exchange.
- Supplier will provide the Data Warehouse Data Model, ETL Layer, and SOV reports creation capability. Supplier will provide the required CMS reports, all reports defined in the SOW, and an additional 2,000 hours a year of support to assist the SOV in formatting and producing reports. For avoidance of doubt, there shall be no additional or incremental charge to SOV for the aforementioned support.
- Supplier's proposed price includes an extract to CMS for Risk Management Corridor Adjustment processes, but the data collection requirements and analysis remain undefined and are not included in CGI's proposed price.

1.2.2.4. Policies, Procedures, and Internal Controls

- The SOV is responsible for developing the internal control policies and executing inter-agency agreements for the Exchange.

1.2.2.5. Training

- Supplier will provide a dedicated Training Manager for the Project. The SOV will designate dedicated Project leads to support Change Management and Outreach activities. The SOV Change Management and Outreach Project leads and the Supplier Training Manager will coordinate activities to support the timely completion of tasks identified in the Project Work Plan.
- Supplier will provide and deliver Trainer curriculum. Training activities will occur within the State of Vermont. The SOV will provide adequate and appropriately skilled staff to serve in the role as Trainers.
- The SOV will assist in identification of roles, positions, audience groups and the training requirements for each role and position. It is assumed that learners will participate in the training events identified in the Project Work Plan.
- Supplier shall provide and maintain the rooms and the necessary equipment and resources to accommodate, support and deliver training in a variety of methods including instructor led and computer based training, online tutorials, and podcasts.

1.2.3. Deliverable List

Project Management Deliverables

Deliverable	Description
(D-04) Project Management Plan (PMP)	Project overview, project scope definition, overview of the project management plan and related processes. Includes a project organization chart. The PMP includes the following standard sections.
Scope Management Plan	The Scope Management Plan addresses the definition, monitoring, controlling, verification and communication of project scope to stakeholders and team members. Contractual documents, the project deliverables list, and the work breakdown structure provide the definition of scope for the projects, and this document describes the roles, processes and tools used to manage this scope, particularly as it relates to how and when scope changes may be made in the Change Management topic. Change Management will describe the process, procedures, and tools that will be employed for the project to determine whether or not a change should be made to a baseline configuration item. The Change Management process provides the capability to identify, accept, evaluate, determine, and communicate the disposition of issues that result in changes to project scope or configured items.
Configuration Management Plan	The processes and tools by which software and non-software work products are developed, stored, reviewed, approved, versioned, baselined, tracked, and maintained. This includes deliverables management and requirements traceability. This will cover both the management of deliverables and requirements through the project lifecycle, and address the tools and processes for managing them.
Schedule Management Plan	The process of managing, maintaining and controlling the Project Work Plan and Schedule, including a WBS based upon deliverables and milestones of the Project
Quality Management Plan	The overall quality methodology and processes for the project, including quality assurance, quality management, and quality control. The Quality Management Plan addresses the methodology for quality, including adherence to project standards, templates, processes and procedures. This section will specifically address the processes by which project deliverables will be clearly defined, including acceptance criteria, through Deliverable Expectation Documents (DED), followed by other process steps in place to maintain quality as deliverables are developed, submitted, reviewed and approved.
Human Resources Management Plan	The processes that are used to organize and manage the project team. It includes the approach for addressing staffing requirements, project roles, and responsibilities and how changes in staffing will be handled.

Deliverable	Description
Communication Management Plan	The processes required to ensure timely and appropriate collection and distribution of project information. It also includes the methodology for determining the information needs of project stakeholders, how necessary information will be made available to stakeholders in a timely manner, and how performance reporting will be distributed to ensure successful project communication to all levels of stakeholders. This section will clearly address Project status reporting and will describe the intervals for formalized written and verbal reporting on project progress against the project schedule, keeping project stakeholders informed on critical aspects of project health such as schedule, issues, scope, resources, allowing management to take action to address issues and risks. Supplier is integrating the HBE Project status reporting with the processes being developed and implemented by the SOV, both in terms written status and status meetings and presentations.
Risk Management Plan	The processes concerned with conducting risk management planning, identification, analysis, responses and monitoring and control on a project including tracking tools. The objective of Risk Management is to decrease the impact and probability of adverse events on the project.
Issue Management Plan	Identification, inventory, analysis, responses, monitoring, and control of issues on the project including tracking tools. The objective of Issue Management is to identify and address issues that have occurred, or will occur.
Contract Management Plan	Provides visibility and transparency and addresses how Supplier will identify, track, and report on contract terms and conditions to demonstrate how and when they are fulfilled and invoices will be issued. The approach to contract management also includes management and administration of Supplier subcontracts. This section will address performance management, and will describe the methods for performance goal establishment, data collection, analysis, control, and reporting. This will also include tracking and report of Supplier monies earned based on the Services provided and Deliverables furnished as well as supporting payment processes. This will also include processes for establishing and tracking the formal deliverables list.
(D-01) Baseline Schedule (WBS)	Supplier has provided and will maintain a WBS in MS Project that provides: o A consolidated view of the activities, activity descriptions, and activity durations o A list of deliverables tied to project milestones o A way to track the project schedule against the planned schedule o Deliverable approval periods The WBS will be maintained throughout the life of the project and will be updated as necessary (weekly at a minimum) to reflect the accurate status of the project. For convenience, the WBS is also referred to as the "Work Plan," "Project Work Plan," "Schedule" and "Project Schedule" herein.

Elaboration Deliverables

Deliverable	Description
Interface Design Documents	Supplier will develop interface requirements documents to support the 4 categories of interfaces listed. The interface requirements documents will address for each of the interfaces the major function being supported, direction (one or two way), the major integration points, a specific list of the data elements, and the frequency (batch or interactive).
(D-05) State Interfaces Design Document	Specific requirements for the state interfaces design.
(D-06) Federal Interface Design Document	Specific requirements for the federal interfaces design.
(D-07) Carrier System Interface Design Document	Specific requirements for the carrier interfaces design.
(D-08) Exchange Accounting System Interface Design Document	Specific requirements for the accounting system interfaces design.
Deliverable: (D-17) Requirements Specification Document (RSD)	The RSD provides a complete description of the behavior of the system to be implemented as well as describe interactions the users will have with the software. Supplier will again leverage the documentation provided by the Federal CALT and our own artifacts from HIX projects already underway.
(D-16) Requirement Traceability Matrix (RTM)	The Requirements Traceability Matrix, which for avoidance of doubt includes the Functional Requirement Traceability Matrix and the Non-Functional Requirement Traceability Matrix, is the basis for making sure we meet all the program requirements by Phase. It tracks all requirements through the DDI phase to confirm the final solution meets expectations. The RTM provides links between the business requirements, technical design, use cases, and test cases. The RTM validates full coverage of the requirements in the solution and also is the base for analyzing the impact of changing requirements, once in production, to the various system components. The RTM will be updated throughout all phases of program.

Deliverable	Description
(D-18) Test Plan	Plan for testing activities, periods, test cases, mapping requirements to the specific tests, tracking and resolving issues, verification methods, test data needs, and version control. Maps requirements to test cases. Identifies requirements for the testing environment where test cases will be executed. The test plan will include a plan for an end-to-end integration test from end-consumer to all systems and back, testing all federal and state agencies, as appropriate, to ensure accurate Exchange functionality and data
(D-19) Business Rules	Business rules establish how the system will act based on the information presented. Business rules codify State, Federal, and Connector policy into system actions. Business rules will be codified in the Oracle Policy Automation tool. Changes to business rules will follow a similar methodology to other system changes (e.g., analysis and testing) but will be managed by authorized end users.
(D-21) Database Design Document	The Database Design Document will include the system context and the basic database design approach, including dependencies and interfaces with other databases and/or systems. It describes the logical data model, including a definition of common understanding of business data elements and inter-relations to form the basis for physical database design, and physical data model including the database entities/tables/views.
(D-20) System Design Document	Transformation of the requirements, user-oriented functional design, and data design into more technical specifications from which the system will be built.
(D-22) Data Management Plan	Strategy for managing data during and after project execution. Identifies data archiving/data retention plans The goal of a data management plan is to consider the many aspects of data management, metadata generation, data preservation, and analysis to help ensure that data are well-managed in the present, and prepared for preservation in the future and the database schemas support accurate data usage.
(D-23) Interface Control Document (ICD)	Describes external inputs to and all outputs from a system for some potential or actual user of the system. There will be an ICD for each interface that defines the data elements in the interface, the method of transfer, frequency, and contingency plans in the even the interface fails. The Supplier will provide its expertise with the ICD process underway for the Federal HUB and will use our HIX Center of Excellence and our current projects to inform the SOV HBE project.

Construction Deliverables

	Description
(D-26) System Security Plan	Required of federally owned systems. This plan describes security controls within the system that will protect the confidentiality, integrity, and availability of the system and its information.

	Description
Deliverable: (D-27) Information Security Risk Assessment	Required for federally owned systems. This assessment includes identification of risks and possible mitigation associated with information security components and supporting infrastructure.
Deliverable: (D-28) Implementation Plan	Descriptions and procedures of how the Exchange solution will be installed, deployed, and transitioned into an operational system The Implementation and Deployment Plans must include the following components: A detailed explanation of the Supplier's implementation methodology An up-to-date detailed implementation schedule
Deliverable: (D-29) Contingency/Recovery Plan	Required of federally owned systems. Includes management policies and procedures to maintain or restore business and technical operations in the event of emergency, system failure, or disaster
Deliverable: (D-30) Data Use Agreement/Data Exchange Agreement/Interconnection Security Agreement	Agreements between parties for the use of personal identifiable data, and to ensure secure data exchange. This includes a Safeguards Procedures Report (SPR), which includes information that Internal Revenue Service (IRS) Office of Safeguards expects from an agency regarding their procedures for safeguarding Federal Tax Information (FTI), in any instance where that agency intends to receive, store, process, or transmit FTI

Test Results Deliverables

Each system test scenario will be executed and the results recorded and compared with expectations. Any mismatch between expected and actual results will be recorded as a possible defect. Test results will include test performance and outcomes identifying any issues in any process from beginning to end as needed to ensure accurate Exchange functionality.

Deliverable	Description
(D-09) Eligibility System Interface Test Results	Test results for the Eligibility System Interface
Deliverable: (D-10) Other State Interfaces Test Results	Test results for the Other State Interfaces
Deliverable: (D-11) Federal Exchange Eligibility Service Interface Test Results	Test results for the Federal Exchange Eligibility Interface
Deliverable: (D-12) CMS System Interface Test Results	Test results for the CMS System Interface
Deliverable: (D-13) Federal Hub Interface Test Results	Test results for the Federal Hub Interface
Deliverable: (D-14) Carrier System Interface Test Results	Test results for the Carrier System Interface
Deliverable: (D-15) Carrier System Interface Test Results	Test results for the Carrier System Interface

Deliverable: (D-31) Test Reports	This deliverable will include the test results for the following 4 test cycles • Integration Test Reports • Performance Test Reports • System Test Reports • UAT Test Reports Though the deliverable will include all 4 test cycles, the cycle specific reports will be developed and reviewed incrementally throughout the testing cycle.

Transition and Support Deliverables

	Description
Deliverable: (D-32) Go-Live Document	Documentation in support of the Exchange Go-Live Event.
Deliverable: (D-33) Operation & Maintenance Manual (O&M)	Description of the business product operating in the production environment, and information necessary to effectively handle routine production processing, ongoing maintenance, performance monitoring, and identification of problems, issues, and/or change requirements.
(D-34) Training Plan	Description of training effort to use and support the system, including initial and subsequent remedial training for business users and system support personnel.
(D-24) Training Materials	Documentation on the overall solution to enable end users to effectively utilize the system. Documentation associated with the deployment and use of the Business Product, including instructor and student guides, audio-visual aids, and computer-based or other media. The Supplier Team will leverage our other HIX engagements to bring together the Training Materials, Manuals and lessons learned.
(D-25) User Manuals	Documentation associated with the deployment and use of the Business Product, including instructor and student guides, audio-visual aids, and computer-based or other media.

1.3. SOV Quality Assurance (QA) / Independent Verification and Validation (IV&V) Vendor Support

Quality Assurance (QA) is a review process performed by an organization that is technically, managerially, and financially independent of the vendor organization. SOV understands the importance and strongly endorses the use of QA to ensure a successful System. SOV will contract for QA services to support the success of the Project. QA and project oversight activities related to the project will be performed by the Quality Assurance provider that has been selected by SOV.

QA Verification uses iterative processes throughout the SDLC to determine whether the plans, methods and products delivered fulfill the requirements placed on them by previous iterations, phases and steps and are internally complete, consistent, and sufficiently correct to adequately support the next iteration, phase and step.

QA Validation is the process of examining and exercising the complete application (software, hardware, procedures, and documentation) to determine whether all stakeholders' requirements have been met. QA Validation begins at the beginning of the SDLC phase and deliverable to ensure that the plan and approach will move in a direction to eventually satisfy stakeholder needs. QA Validation also occurs at the end of the SDLC phase and deliverable to ensure the deliverable truly meets the latest requirements of the stakeholders (regardless of how many times these requirements may have changed during the project)

Supplier will collaborate with the current SOV QA/IV&V vendor in partnership with the State and the SOV and Supplier Project Directors and perform the following functions:

- Review project planning deliverables to ensure they are sufficient and meet applicable project standards
- Review ongoing project processes, methods and activities
- Provide technical review and verification of key project milestones and deliverables
- Provide independent review of project deliverables against requirements
- Anticipate and identify project risks and monitor the project risk management process
- Offer suggestions for problem and issue resolution
- Develop Independent Project Oversight Reports and delivers them to the Executive Committee and Project Management team
- Provide monthly review and recommendations to the Executive Committee regarding project status and risk anticipation, prevention and mitigation
- Provide periodic review and recommendations to the Project Director regarding project status and risk anticipation, prevention and mitigation

1.4. State of Vermont Health Services Enterprise Program Office of IT Projects Structure

State of Vermont Health Services Enterprise Program Office of IT Projects

AHS and Department of Information and Innovation Project Roles and Responsibilities

Role	Functions
Project Sponsor	The Project Sponsor assumes project ownership and performs the following functions: Assumes project ownership, and is the highest possible level of project review and provides policy leadership and oversight as needed. Reviews and resolves policy, fiscal, and resource allocation issues that cannot be resolved at lower levels. Ultimately accountable for securing spending authority and resources. Acts as a vocal and visible champion, legitimizing goals and objectives.
Executive Committee	The Executive Committee will be comprised of senior management personnel and representation from the Project facilitated by an appointed chair person who will be part of the committee, and the committee will convene regularly to provide direction or support required to the project and to support the Project Director.
Project Director	The Project Director is responsible for the overall success of the project through planning, directing, and overseeing the activities of the Project resources.
Project Team	The Project Team will be comprised of the various SMEs from both the business and technical spheres and end users from the State, and Local Agencies, as well has QA team members. This team will assist in various day- to-day activities and/or key milestones of the project.
Project Manager	The Project Manager will be responsible for gathering and distributing information on project status, risks, issues and quality assurance reporting. This role will be filled by a person with in- depth knowledge of State and Industry PM methodologies and will report to the Project Director. The Project Manager will have the responsibility of formally accepting vendor project deliverables, unless this responsibility is delegated to another party. The Project Manager will be responsible from a State perspective for ensuring scope, schedule, budget, and minimal required documentation deliverables are completed.

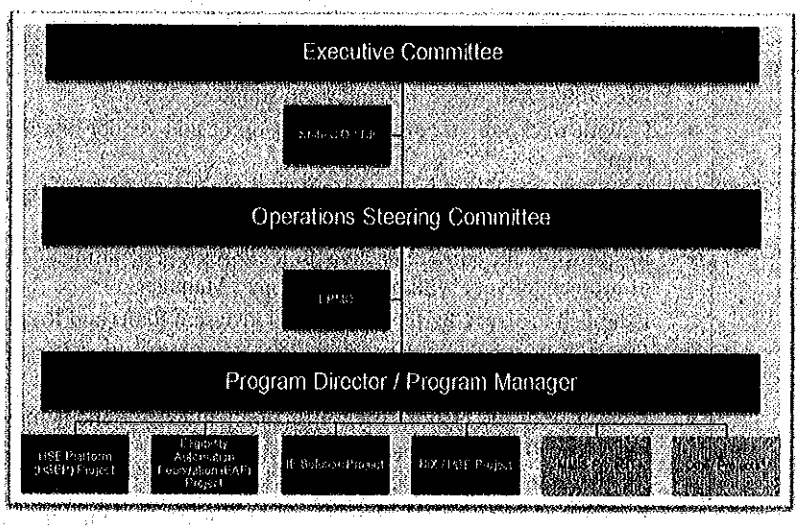
Role	Functions
Business Leads	The HBE Business Leads will work with their respective SMEs of the business units to understand their System and process requirements and articulate the requirements to the Supplier, Integration Managers, QA Lead and the Technical Leads. The person in this role ensures that the proposed solution aligns with the business requirements of the organization. He or she will have the ability to manage the expectations of the business units with a clear understanding of the Project Sponsor's project objectives. This role will be filled by an FTE with in-depth knowledge about the business side of Eligibility and will report to the respective Integration Manager.
Technical Leads	The HBE Technical Leads are responsible for the successful implementation and execution of the proposed solution. Responsibility includes managing the technical resources assigned to support the project. He or she will be responsible for all technical aspects of the project and working with enterprise architects.
State CIO (Department of Information and Innovation)	The Department of Information and Innovation was created in2003 to provide direction and oversight for all activities directly related to information technology within state government, including telecommunications services, information technology equipment, software, accessibility, and networks in state government. The CIO and Commissioner of DII have broad authority to meet the goals of the department as established by statute and policy. The CIO has approval authority for all IT activities in excess of $100k.
Enterprise Project Management Office	The EPMO provides statutory oversight of IT projects within the State, develops and maintains project management artifacts, implements standards for IT project selection, ensures benefit realization of IT projects and manages the State IT project portfolio. It will provide oversight and guidance for the State Project Manager, project management team and Supplier Project Managers.
QA Leads	Quality Assurance (QA) Lead is responsible for ensuring that all System components are error-free and meet Project's expected level of Quality. Responsibility includes defining and managing the QA process throughout the SDLC (System, Integration, UAT, Formal Acceptance Testing (FAT) and Pilot Testing) and managing various QA resources at each phase of Testing as defined in the Test Plan (D-18).
Business SMEs	Business SMEs from all involved business units will be asked to participate in the requirements definition process, data cleansing, QA and testing and training efforts. Business SMEs will be utilized on an as-needed basis and at key milestones of the project.
Technical SMEs	Technical SMEs from all involved IT units will be asked to participate in the non-functional requirements, design, and data conversion, QA and testing and training efforts. Technical SMEs will be utilized on an as needed basis and at key milestones of the project.

Health Services Enterprise (HSE) Program Management Office Structure and Responsibilities

The following Figure describes the current structure of the HSE Program Management Office within AHS.

Due to the interlocking functionality of the projects, each project team will be highly informed of the activities happening within the other projects within the EPMO. The Supplier will be expected to support AHS Program-level and inter-project communications between project teams to ensure proper transfer of knowledge between them.

HSE Program Management Office



State of Vermont Program Management Office Roles and Responsibilities

The following table provides the anticipated roles in the Project organization:

Entity	Core Focus
Executive Committee	• Set Program Mission and Goals • Establish Priorities and Non-Negotiable (Mandates) • Review, Comment and Approve Operations Steering Committee
Operations Steering Committee	• Ensure clarity of business imperatives and alignment of project plans with Executive Committee mandates and statutory authority • Provide oversight of core projects' resource and vendor allocation plans • Review and respond to project risk and risk mitigation strategies that may be escalated to the Executive Committee
Program Director	• Responsible for comprehensive project/program planning and coordination of project delivery with projects' Project Managers • Establish Project Charters, Integrated Program Plans and Roadmap • Ensure coordination effectiveness of the core projects with associated business process changes • Accountable and responsible for fulfilling mandates and achieving key HSE PMO milestones and objectives • Identify and Mitigates HSE PMO Risks • Support resource management by assigning and aligning project managers and team members to the core projects • Provide and fosters open and active communications with all stakeholders
Program Manager	• Accountable and responsible for individual core project planning, implementation and risk identification/mitigation • Support development of Project Charters, Integrated Program Plans • and Roadmap in coordination with Program Director • Responsible for cross project coordination with other core projects and associated business process changes • Accountable for accomplishing the stated project objectives and management of vendors assigned to the individual projects
Project Manager	• Accountable and responsible for individual core project planning, implementation and risk identification/mitigation • Responsible for cross project coordination with other core projects and with related Business Process Reengineering Projects • Accountable for accomplishing the stated project objectives and management of vendors assigned to the individual projects
Business Lead	• Ensure active involvement of Business SMEs in core project • Lead coordination efforts between core project and related BPR efforts
Technical Lead	• Ensure active involvement of Technical SMEs in core project • Ensure technical standards and State policy is followed through projects • Coordinate technical efforts with Program and State technical leadership
Subject Matter Experts (SMEs)	• Responsible for input within their areas of expertise • Contribute to deliverables

1.5. Supplemental Activities

As an output of the Revised Scope Date item resolution, CGI will undertake the following supplemental activities:

Customer Service

- Provide SME resource(s) to liaison between CGI and Customer Support workshops; identify potential improvement opportunities
- Assist in analyzing the current set of Resolver roles and responsibilities, ecosystem, and escalation points, and recommend customer-centric and efficient best practices
- The CGI SME will also provide guidance for Operating Level Agreements by reviewing and commenting on key focus areas, including services provided, escalation procedures, change procedures and process improvement

Financial Management

- Utilizing existing templates, design, build and implement reports based on financial data received from the Premium Processing solution
- All reports will be available for automatic upload into VISION on a daily basis
- Three reports have been identified for development, AR, AP and GL, with an additional two more to be defined

Privacy & Security

The following items will be included as part of CGI's project delivery:

- Draft PIA
- Draft a Business Partner Agreement
- Draft standards, policies and procedures to comply with 45 CFR §155.260
- Design training for staff (ESD etc.) re ACA requirements. (mandatory HIPAA training already in place)
- Design training for contractors – for example navigators and/or assistors, with the final list to be developed.

User Experience

- Should SOV chose, contract with Jellyvision for the implementation of their avatar solution, supporting the non-transaction member experience
- At the direction of SOV, engage additional resources to support the activities in the areas of user experience, member quality assessment, and/or decision support tools

The following adjustments were made to the cost proposal based on the output of the 30 Day activities

- A collective goal was set to identify and act upon potential re-use opportunities, reflected as a credit to SOV
- Plan Management implementation costs were reduced
- Costs for an interface with the Federal Data Hub were added
- Requirements in support of MAGI Medicaid were added to the RTM

ATTACHMENT 4
Exhibit L

[see attached]

1 Executive Summary

CGI's Cost Proposal to the Hawaii Health Connector was used as the basis for the State of Vermont Health Benefit Exchange cost workbook. The following is a high-level comparison of the two sets of cost schedules, with the Vermont figures reflecting those in the Amended and Restated Exhibit L, Cost Proposal.

Description of Deliverable	Vermont	Hawaii
Project Planning & Administration Deliverables	$2,460,650.00	$2,801,683.70
Design, Development & Implementation Deliverables	$14,227,105.00	$14,250,913.67
Full Implementation of Exchange Solution[1]	$28,935,393	$21,801,580.81
Total Detailed Deliverable Cost Schedules	**$45,623,148**	**$38,854,178.18**
Ongoing Operation Costs – Base Years	$10,206,027.00	$14,441,125.64
Ongoing Operation Costs – Optional Years	$13,782,240.00	$9,565,674.50
Rate Card – *Evaluation only amount from HI HIX RFP*	$ 0.00	$275,392.56
Mandatory Optional Costs	$0.00	$8,343,133.00
Grand Total	**$69,611,415.00**	**$71,479,503.88**

Some of the more significant areas of cost differences between the Vermont and Hawaii cost proposals include:

- Salary Adjustments to reflect competitive nature of market for qualified project team members.
- Dedicated Hosting Solution
- Software License Savings through the removal of Oracle and Healthation licenses.
- Software Maintenance Savings
- Exeter IP & Services
- Reduced Contract Term

[1] Definition in Hawaii cost proposal included '(with Premium Processing for SHOP)'

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

1.1 Cost Proposal

CGI has carefully constructed a cost effective proposal to design, develop, implement and operate a Health Insurance Exchange system (the "Exchange") to facilitate access to affordable health insurance coverage for all citizens of the State of Vermont in compliance with your RFP requirements.

This section of our proposal includes the costs to implement our solution in compliance of the federal Exchange deadlines, including the October 1, 2013 date for open enrollment and the January 1, 2014 date for full Exchange operations. Our cost proposal is based on the assumption of a base two-year contract plus two one-year options and includes the firm-fixed price one-time fees for the design, development and implementation of the Exchange solution, ongoing fees for fifteen months of mandatory Maintenance and Operations (M&O) and two years of optional M&O.

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

1.2 CGI's Overall Cost Summary

Table 1 summarizes the pricing of our total solution.

Table 1: Mandatory Solution Components

Solution Components	Proposed Price
FFP for Design, Development and Implementation of our Exchange Solution	45,623,148
Maintenance and Operations (total for base contract term + 2 one-year options)	23,988,267
Total Product Price Mandatory Components	0.00
Grand Total Price Mandatory Components	**69,611,415**

The following subsections of our proposal describe the cost elements of our proposed solution. The completed tables can be found in the following sections.

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

1.3 Table 5.2.2 Detailed Deliverable Cost Schedules

This cost schedule provides the firm fixed price for the development, certification and deployment of our Exchange solution. The amounts presented in this section include all services, travel, software, overhead and other costs required for CGI's scope as presented in our proposal.

The values presented in this schedule align with the actual timing of CGI's costs, based on the level of effort associated with each underlying deliverable and the timing of 3rd party software components required over the course of delivery. CGI understands that the basis for the Payment Schedule will be the Payment Deliverables that make up each broad category presented in this table. The discrete Payment Deliverables have been defined in Exhibit L, the revised Cost Proposal.

Worksheet Notes:

- Contract Start date is assumed to be 12/17/2012. A later start may affect price due to the fixed federally mandated key dates for open enrollment and full Exchange operations.
- CGI's proposed price includes an extract to CMS for Risk Management Corridor Adjustment processes, but the data collection requirements and analysis remain undefined and are not included in our proposed price

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

1.4 Table 5.2.3 Ongoing Operations Costs – Base Years

This schedule provides the ongoing Maintenance and Operations costs of our Exchange solution during the two year base contract. The fees include coverage of operations, software maintenance, fulfillment costs and hosting.

Worksheet Notes:

- M&O commences upon the 10/1/2013 go-live date of the Exchange.
- The first year of mandatory M&O runs from 10/1/2013 through 9/30/14.
- To align with the two-year base contact period, the 2nd year of mandatory M&O is only a partial year, running from 10/1/2014 through 12/31/14 and has been priced accordingly.

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

1.5 Table 5.2.4 Ongoing Operations Costs – Optional Years

This schedule provides pricing for the ongoing Maintenance and Operations of our Exchange solution during the two optional years. The fees include coverage of operations, software maintenance, fulfillment costs and hosting.

Worksheet Notes:

- The first optional year of M&O runs from 1/1/2015 through 12/31/2015
- The second optional year of M&O runs from 1/1/2016 through 12/31/2016.

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

1.6 Table 5.2.5 Hourly Rate Schedule for Change Orders

This schedule includes hourly rates for potential Change Orders. The rates in this schedule are for enhancements or other Change Orders in excess of the 2,000 hours already covered in the ongoing M&O fees on Tables 5.2.3 and 5.2.4.

CGI understands that there is no commitment from the SOV to purchase Change Orders.

Worksheet Notes:

- The total value from Table 5.2.5 was included in the Hawaii HIX total evaluated cost amount. The proposed hourly rates were each multiplied by 100 hours in order to provide a meaningful difference between the rates proposed by multiple vendors. This evaluation-only amount does not reflect committed scope that will be delivered by CGI.
- We have provided staff classifications for the major position types we would expect to be delivering incremental Change Orders.

1.7 Table 5.2.6 Summary Schedule of Project Costs

This schedule brings forward the totals from schedules 5.2.2 through 5.2.5.

Worksheet Notes:

- This schedule includes the two optional years of M&O fees in addition to the mandatory costs for the base contract term.

1.8 Tables 5.2.7 through 5.2.8.9

These schedules are not applicable to our Cost Proposal. CGI does not have any "Other Associated Costs" and Vermont has requested that we do not provide pricing for the Mandatory Options that were included in our Hawaii HIX proposal.

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

1.9 Tables 5.2.9.1 through 5.2.9.6

These are the payment schedules as follows:

- Schedule 5.2.9.1 Deliverable Pricing – deliverables are grouped by their corresponding Milestones
- Schedule 5.2.9.2 Milestone Payment Schedule – presents the payments for deliverables by Milestone
- Schedule 5.2.9.3 Monthly Payment Schedule – presents the monthly hosting and maintenance costs during DDI
- 5.2.9.4 License Payment Schedule – provides the list of software products and price. Software will be invoiced on installation
- 5.2.9.5 M&O Payment Schedule – provides the payment schedule during operations
- 5.2.9.6 Payment Schedule Summary – summarizes the payment schedules.

A single invoice will be prepared and presented at the beginning of each month that consolidates all of the payments across the Payment Schedules that are due that month.

© 2012 CGI Technologies and Solutions Inc., All Rights Reserved.
Proprietary and Confidential

Table 5.2.1. COST PROPOSAL IDENTIFICATION AND INSTRUCTIONS

Contents of the cost proposal must be as follows:

1. **Tab I - Title Page**

   The title page must include the following:

   A. Cost Proposal for: ***Vermont Agency for Health Services***

   B. RFP: ***n/a***

   C. Bidder Information:
   - Name: CGI Technologies and Solutions Inc
   - Address:

2. **Tabs 2 - 8 Cost Proposal Details**

   A. Cost proposal must be in the Excel format and follow the tabs included in this template

Vermont HIX

Table 5.2.2. Detailed Deliverable Cost Schedules

RFP Section	Description of Deliverable	Section Number	Cost
5.2.2. Detailed Deliverable Costs Schedules	**Project Planning and Administration Deliverables**	RFP Sections	
	Project Management Plan / Detailed Project Plan	4.4.1 & 4.4.2	$2,460,650.00
	Subtotal for - Planning and Administration		***$2,460,650.00***
5.2.2. Detailed Deliverable Costs Schedules	**Design, Development and Implementation Deliverables**	RFP Sections	
	Requirements Specification Document (RSD) / Requirements Traceability Matrix (RTM)	4.4.3.2 & 4.4.3.3	$5,394,170.00
	Test Management Plan / System Test Results	4.4.3.6 & 4.4.3.7	$8,832,935.00
	Subtotal for Design, Development and Implementation Deliverables		***$14,227,105.00***

Table 5.2.2. Detailed Deliverable Cost Schedules

RFP Section	Description of Deliverable	RFP Section Number	Cost
5.2.2. Detailed Deliverable Costs Schedules	**Full Implementation of Exchange Solution with Premium Processing for SHOP**	RFP Sections	
	Exchange Solution		
	Usage of the GSA Cloud during DDI	4.4.4	$1,240,700.00
	Full Implementation of the Dedicated Vblock Hosting Environment		$4,285,857.00
	Software Licenses		$6,507,109.00
	Software Maintenance through DDI (before commencement of M&O)		$1,453,224.00
	Full implementation of Open Enrollment including Premium Processing for SHOP	4.2	$3,940,930.00
	Full Implementation of Interfaces:	4.2.3	$3,973,825.00
	Department of Health Services Eligibility System		
	Federally Managed Eligibility Service		
	CMS Systems		
	State Insurance Division Systems		
	Issuer Systems		
	Accounting System		
	Scope Changes from 30-day List:		$5,419,777.00
	Completion of Training for Implementation of the Business Operations Solution	4.4.2.15 & 4.4.3.11	$2,113,971.00
	Subtotal for Exchange Solution		***$28,935,393.00***
	Total Detailed Deliverable Cost Schedules		***$45,623,148.00***

Vermont HIX

Table 5.2.3. Ongoing Operation Costs – Base Years

RFP Section	Base Contract Year		Annual Total
5.2.3. Ongoing Operation Costs – Base Years	M&O Base Contract Year 1 Fixed Operations Cost (October 1, 2013 - September 30, 2014)		$6,717,260.00
	M&O Base Contract Year 1 Fixed Software Maintenance Cost (October 1, 2013 - September 30, 2014)		$1,457,282.00
	Total for M&O Base Contract Year 1		$8,174,542.00
	M&O Base Contract Year 2 Fixed Operations Cost (October 1, 2014 - December 31, 2014)		$1,666,120.00
	M&O Base Contract Year 2 Fixed Software Maintenance Cost (October 1, 2014 - December 31, 2014)		$365,365.00
	Total for M&O Base Contract Year 2		$2,031,485.00
	Subtotal		$10,206,027.00
	Sub-Total Evaluated Operations Price for Base Contract Years		***$10,206,027.00***

Table 5.2.4. Ongoing Operation Costs – Optional Years

RFP Section	Optional Contract Year		Annual Total
5.2.4. Ongoing Operation Costs – Optional Years	Optional M&O Contract Year 1 Fixed Operations Cost (January 1, 2015 - December 31, 2015)		$6,193,780.00
	Optional M&O Contract Year 1 Fixed Software Maintenance Cost (January 1, 2015 - December 31, 2015)		$1,062,537.00
	Total for Optional M&O Contract Year 1		$7,256,317.00
	Optional M&O Contract Year 2 Fixed Operations Cost (January 1, 2016 - December 31, 2016)		$5,459,050.00
	Optional M&O Contract Year 2 Fixed Software Maintenance Cost (January 1, 2016 - December 31, 2016)		$1,066,873.00
	Total for Optional M&O Contract Year 2		$6,525,923.00
	Subtotal		$13,782,240.00
	Sub-Total Evaluated Operations Price for Optional Years		***$13,782,240.00***

Table 5.2.5. Hourly Rate Schedule for Change Orders

RFP Section	Staff Classifications	Evaluated Annual Number of Hours for Change Orders — For Evaluation Purposes Only	Hourly Rate	Total Evaluated Change Order Price
5.2.5. Hourly Rate Schedule for Change Orders	Technical Lead/DBA	0	$256.25	$0.00
	Technical Analyst	0	$218.75	$0.00
	Business/Configuration Analyst	0	$206.25	$0.00
	Programmer	0	$193.75	$0.00
	Trainer	0	$206.25	$0.00
	Technical Writer	0	$87.50	$0.00
	Tester	0	$206.25	$0.00
	Security Analyst	0	$218.75	$0.00
	Senior SME	0	$281.25	$0.00
	Technical Architect	0	$331.25	$0.00
	Subject Matter Expert	0	$243.75	$0.00
			Subtotal	$0.00
			Evaluated Total	***$0.00***

Table 5.2.6. Summary Schedule of Project Costs

Reference to RFP Section Number	Summary of Project Costs Through Base Contract Years	Cost
5.2.2	Project Planning and Administration Deliverables	$2,460,650.00
5.2.2	Subtotal for Design, Development and Implementation Deliverables	$14,227,105.00
5.2.2	Subtotal for Exchange Solution	$28,935,393.00
	Sub-Total of Project Tasks	$45,623,148.00
5.2.3.	Sub-Total Evaluated Operations Price for Base Contract Years	$10,206,027.00
5.2.4.	Sub-Total Evaluated Operations Price for Optional Years	$13,782,240.00
	Sub-Total of Operations costs	$23,988,267.00
5.2.5	***Sub-Total Evaluated Change Order Price***	$0.00
	Total Project Costs for Base Contract - not including other associated costs	***$69,611,415.00***

Vermont HIX

RFP Section 5.2.7 Other Associated Costs

Table 5.2.7. Other Associated Costs

Item #	Description of Other Associated Costs	Cost
1	N/A	n/a
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
	SUB-TOTAL	$0.00

Vermont HIX

RFP Section 4.5.1 Call Center Costs

Table 5.2.8.1 Call Center Technology Costs

One-Time Call Center Technology Costs - Not included in the Summary Schedule of Costs		
Hardware:		$0.00
Software		$0.00
Services	Design	$0.00
	Development	$0.00
	Testing	$0.00
	Training	$0.00
	Implementation.	$0.00
	Subtotal	$0.00
	Total One-Time Call Center Cost Information	***$0.00***

Vermont HIX

RFP Section 4.5.4 Medicaid Plan Selection through the Exchange Solution

Table 5.2.8.2 Medicaid Plan Selection through the Exchange Solution Costs

One-Time Medicaid Plan Selection Costs - Not Included in the Summary Schedule of Costs		
Services	Design	$0.00
	Development	$0.00
	Testing	$0.00
	Training	$0.00
	Implementation.	$0.00
	Subtotal	$0.00
	Total One-Time Medicaid Plan Selection Costs	***$0.00***

Vermont HIX

RFP Section 4.5.4 Medicaid Plan Selection through the Exchange Solution

Table 5.2.8.2 Medicaid Plan Selection through the Exchange Solution Costs

Ongoing Maintenance of the Medicaid Plan Selection Application Costs - Not included in the Summary Schedule of Costs	
Base Contract - Application Maintenance	
Base Contract Year 1 (October 1, 2013 to September 30, 2014)	$0.00
Base Contract Year 2 (October 1, 2014 to September 30, 2015)	$0.00
Base Contract Year 3 (October 1, 2015 to September 30, 2016)	$0.00
Subtotal	$0.00
Total Base Contract Medicaid Plan Selection Application Maintenance	**$0.00**
Optional Contract - Application Maintenance	
Optional Contract Year 1 (October 1, 2016 to September 30, 2017)	$0.00
Optional Contract Year 2 (October 1, 2017 to September 30, 2018)	$0.00
Subtotal	$0.00
Total Optional Contract Medicaid Plan Selection Application Maintenance	**$0.00**
Total Ongoing Medicaid Plan Selection Costs	***$0.00***

Vermont HIX

RFP Section 4.5.1 Call Center Staffing and Operations - Base Years Costs

Table 5.2.8.4 Call Center Staffing and Operation - Base Years Costs

Base Contract Year 1 (October 1, 2013 - September 30, 2014)

Program	Shift	Call Center Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Annual Costs
Exchange	Prime	Call Center Manager	n/a	n/a	n/a	$0.00
		Call Center Representative	n/a	n/a	n/a	$0.00
	2nd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
	3rd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
					Exchange Subtotal	**$0.00**
		Operational Staffing Classification	**Number of Staff**	**Estimated Annual Hours per Staff**	**Hourly Rate**	
		n/a				$0.00
		Operational Costs	**Type of Service**	**Cost Per Month**		
		Supplies & Space Allocation	Call Center facility	n/a		$0.00
					Operational Costs Subtotal	**$0.00**
		Total Call Center - Base Contract Year 1 - Costs				***$0.00***

Vermont HIX

RFP Section 4.5.1 Call Center Staffing and Operations - Base Years Costs

Table 5.2.8.4 Call Center Staffing and Operation - Base Years Costs

Base Contract Year 2 (October 1, 2014 - September 30, 2015)

Program	Shift	Call Center Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Annual Costs
Exchange	Prime	Call Center Manager	n/a	n/a	n/a	$0.00
		Call Center Representative	n/a	n/a	n/a	$0.00
	2nd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
	3rd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
					Exchange Subtotal	**$0.00**
		Operational Staffing Classification	**Number of Staff**	**Estimated Annual Hours per Staff**	**Hourly Rate**	
		n/a				$0.00
		Operational Costs	**Type of Service**	**Cost Per Month**		
		Supplies & Space Allocation	Call Center facility	n/a		$0.00
					Operational Costs Subtotal	**$0.00**
		Total Call Center - Base Contract Year 2 - Costs				***$0.00***

Base Contract Year 3 (October 1, 2015 - September 30, 2016)

Vermont HIX

RFP Section 4.5.1 Call Center Staffing and Operations - Base Years Costs

Table 5.2.8.4 Call Center Staffing and Operation - Base Years Costs

Program	Shift	Call Center Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Estimated Costs
Exchange	Prime	Call Center Manager	n/a	n/a	n/a	$0.00
		Call Center Representative	n/a	n/a	n/a	$0.00
	2nd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
	3rd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
					Exchange Subtotal	**$0.00**
		Operational Support Classification	**Number of Staff**	**Estimated Annual Hours per Staff**	**Hourly Rate**	
		n/a				$0.00
		Operational Costs	**Type of Service**	**Cost Per Month**		
		Supplies & Space Allocation	Call Center facility	n/a		$0.00
					Operational Costs Subtotal	**$0.00**
		Total Call Center - Base Contract Year 3 - Costs				***$0.00***

Table 5.2.8.5 Call Center Staffing and Operation - Optional Years Costs

RFP Section 4.5.1 Call Center Staffing and Operations - Optional Years Costs

Optional Contract Year 1 (October 1, 2016 - September 30, 2017)

Program	Shift	Call Center Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Annual Costs
Exchange	Prime	Call Center Manager	n/a	n/a	n/a	$0.00
		Call Center Representative	n/a	n/a	n/a	$0.00
	2nd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
	3rd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
					Exchange Subtotal	**$0.00**
		Operational Staffing Classification	**Number of Staff**	**Estimated Annual Hours per Staff**	**Hourly Rate**	
		n/a				$0.00
		Operational Costs	**Type of Space**	**Cost Per Month**		
		Supplies & Space Allocation	Call Center facility	n/a		$0.00
					Operational Costs Subtotal	**$0.00**
		Total Call Center - Optional Contract Year 1 - Costs				***$0.00***

Table 5.2.8.5 Call Center Staffing and Operation - Optional Years Costs

RFP Section 4.5.1 Call Center Staffing and Operations - Optional Years Costs

Optional Contract Year 2 (October 1, 2017 - September 30, 2018)

Program	Shift	Call Center Staffing Classification	Number of Seats	Estimated Annual Hours per Seat	Hourly Rate	Annual Costs
Exchange	Prime	Call Center Manager	n/a	n/a	n/a	$0.00
		Call Center Representative	n/a	n/a	n/a	$0.00
	2nd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
	3rd Shift	Call Center Representative	n/a	n/a	n/a	$0.00
					Exchange Subtotal	**$0.00**
		Operational Staffing Classification	**Number of Seats**	**Estimated Annual Hours per Seat**	**Hourly Rate**	
		n/a				$0.00
		Operational Costs	**Type of Space**	**Cost Per Month**		
		Supplies & Space Allocation	Call Center facility	n/a		$0.00
					Operational Costs Subtotal	**$0.00**
		Total Call Center - Optional Contract Year 2 - Costs				***$0.00***

Vermont HIX

RFP Section 4.5.3 Premium Billing Operations - Base Years Costs

Table 5.2.8.7 Individual Premium Billing Operations - Base Years Costs

Base Contract Year 1 (October 1, 2013 - September 30, 2014)

Premium Billing Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Annual Costs
PB Business Analyst	n/a	n/a	n/a	$0.00

Operations Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	
n/a				$0.00

Operations Costs	Type of Service	Cost Per Month	

Total Premium Billing Operations - Base Contract Year 1 - Costs ***$0.00***

Vermont HIX

RFP Section 4.5.3 Premium Billing Operations - Base Years Costs

Table 5.2.8.7 Individual Premium Billing Operations - Base Years Costs

Base Contract Year 2 (October 1, 2014 - September 30, 2015)

Premium Billing Staffing Classification	Number of Staff	Estimated Hours per Staff	Hourly Rate	Annual Costs
PB Business Analyst	n/a	n/a	n/a	$0.00
Operational Staffing Classification	**Number of Staff**	**Estimated Hours per Staff**	**Hourly Rate**	
n/a				$0.00
Other Operational Costs	**Description of Service and Cost per Month**			

Total Premium Billing Operations - Base Contract Year 2 - Costs ***$0.00***

Vermont HIX

RFP Section 4.5.3 Premium Billing Operations - Base Years Costs

Table 5.2.8.7 Individual Premium Billing Operations - Base Years Costs

Base Contract Year 3 (October 1, 2015 - September 30, 2016)

Premium Billing Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Annual Costs
PB Business Analyst	n/a	n/a	n/a	$0.00

Operational Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	
n/a				$0.00

Operational Costs	Operational Services Cost Per Month	

Total Premium Billing Operations - Base Contract Year 3 - Costs ***$0.00***

Vermont HIX

RFP Section 4.5.3 Premium Billing Operations - Optional Years Costs

Table 5.2.8.8 Individual Premium Billing Operations - Optional Years Costs

Optional Contract Year 1 (October 1, 2016 - September 30, 2017)

Premium Billing Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Annual Costs
PB Business Analyst	n/a	n/a	n/a	$0.00

Operational Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	
n/a				$0.00

Operational Costs	Type of Service	Cost Per Month

Total Premium Billing Opertions - Optional Contract Year 1 - Costs ***$0.00***

RFP Section 4.5.3 Premium Billing Operations - Optional Years Costs

Table 5.2.8.8 Individual Premium Billing Operations - Optional Years Costs

Optional Contract Year 2 (October 1, 2017 - September 30, 2018)

Premium Billing Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	Annual Costs
PB Business Analyst	n/a	n/a	n/a	$0.00

Operational Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	
n/a				$0.00

Operational Costs	Type of Service	Cost Per Month

Total Premium Billing Operations - Optional Contract Year 2 -Costs ***$0.00***

Table 5.2.8.9 Summary Schedule of Mandatory Optional Costs

Section Reference	Summary of Mandatory Optional Costs	Cost
5.2.8.1	Call Center Technology Costs	$0.00
5.2.8.2	Medicaid Plan Selection Costs	$0.00
	Sub-Total of Mandatory Optional One-Time Costs	$0.00
5.2.8.2	Medicaid Plan Selection Application Maintenance - Base Year Costs	$0.00
5.2.8.2	Medicaid Plan Selection Application Maintenance - Optional Years Costs	$0.00
	Sub-Total of Mandatory Optional Medicaid Plan Selection Application Maintenance Ongoing Costs	$0.00
5.2.8.4.	Call Center Operations - Base Years Costs	$0.00
5.2.8.5	Call Center Operations -Optional Years Costs	$0.00
	Sub-Total of Mandatory Optional Call Center Operations Ongoing Costs	$0.00
5.2.8.7	Premium Billing Operations - Base Years Costs	$0.00
5.2.8.8	Premium Billing Operations -Optional Years Costs	$0.00
	Sub-Total of Mandatory Optional Premium Billing Operations Ongoing Costs	$0.00
	Total Mandatory Optional Costs	***$0.00***

Vermont HIX

5.2.9.1 Deliverable Pricing

UID	Deliverable	Finish	Price	Total Resource First Year Deliverable Value	$32,136,258
3881	Deliverable: (D-02) Project Management Plan	2/8/2013	$1,285,450		
3871	Deliverable: (D-01) Baseline Schedule (WBS)	1/16/13	$1,285,450		
	Group 1			**$2,570,901**	
4751	Deliverable: (D-03) State Interfaces Design Document	4/12/13	$321,363		
4762	Deliverable: (D-04) Federal Interface Design Document	4/12/13	$964,088		
4781	Deliverable: (D-05) Carrier System Interface Design Document	4/12/13	$642,725		
4791	Deliverable: (D-06) Exchange Accounting System Interface Design Document	4/12/13	$321,363		
4885	Deliverable: (D-14) Requirement Traceability Matrix (RTM)	4/12/13	$1,285,450		
4877	Deliverable: (D-15) Requirements Specification Document (RSD)	4/25/13	$1,285,450		
4911	Deliverable: (D-21) Interface Control Document	5/1/13	$642,725		
4579	Deliverable: (D-32) Training Plan	5/22/13	$964,088		
4903	Deliverable: (D-19) Database Design Document	5/8/13	$642,725		
4167	Deliverable: (D-20) Data Management Plan	5/8/13	$642,725		
4095	Deliverable: (D-16) Test Plan	5/9/13	$964,088		
4150	Deliverable: (D-17) Business Rules	5/9/13	$642,725		
4895	Deliverable: (D-18) System Design Document	5/9/13	$1,285,450		
	Group 2			**$10,604,965**	
4803	Deliverable: (D-07) Eligibility System Interface Test Results	6/25/13	$642,725		
5339	Deliverable: (D-08) Other State Interfaces Test Results	6/25/13	$642,725		
5178	Deliverable: (D-09) Federal Exchange Eligibility Service Interface Test Results	6/25/13	$321,363		
5210	Deliverable: (D-10) CMS System Interface Test Results	6/25/13	$321,363		
5242	Deliverable: (D-11) Federal Hub Interface Test Results	6/25/13	$964,088		
5274	Deliverable: (D-12) Carrier System Interface Test Results	6/25/13	$964,088		
5306	Deliverable: (D-13) Exchange Accounting System Interface Test Results	6/25/13	$321,363		
5037	Deliverable: (D-26) Implementation Plan	7/22/13	$1,285,450		
5046	Deliverable: (D-27) Contingency / Recovery Plan	7/22/13	$1,285,450		
5055	Deliverable: (D-28) Data Use Agreement/Data Exchange Agreement/Interconnection Security Agreement	7/22/13	$1,285,450		
	Group 3		$0	**$8,034,065**	
4569	Deliverable: (D-31) Operation & Maintenance Manual (O&M)	9/10/2013	$1,285,450		
5063	Deliverable: (D-29) Test Reports	9/18/13	$1,606,813		
4588	Deliverable: (D-22) Training Materials	9/30/13	$1,606,813		
4993	Deliverable: (D-23) User Manuals	9/30/13	$1,606,813		
5001	Deliverable: (D-24) System Security Plan	9/30/13	$1,606,813		
5009	Deliverable: (D-25) Information Security Risk Assessment	9/30/13	$1,606,813		
4545	Deliverable: (D-30) Go-Live Document	11/7/13	$1,606,813		
	Group 4			**$10,926,328**	
			$32,136,258	**$32,136,258**	

Group 1

Milestone: V1 Milestone 1-PM Exchange Components Functional Verification Complete	4/5/13	

Milestone: VT Milestone 2: E&E Exchange Components Functional Verification Complete	4/5/13
Milestone: VT Milestone 3: FM Exchange Components Functional Verification Complete	4/5/13
Milestone: VT Milestone 4: Consumer Assistance Functional Verification Complete	4/5/13
Group 2	
Milestone: VT Milestone 5: Initial PM Exchange Components Development Complete	6/3/13
Milestone: VT Milestone 6: Initial FM Development Complete	6/3/13
Milestone: VT Milestone 7: Initial E&E Development Complete	6/3/13
Milestone: VT Milestone 8: Initial CA Development Complete	6/3/13
Milestone: VT Milestone 10: Connectivity Established for CMS Federal Hub Servics	6/3/13
Milestone: VT Milestone 11: Hub Service and partner testing Complete	6/3/13
Group 3	
Milestone: VT Milestone 12: Communications and Security Testing of Federal Hub Services Review Complete	6/14/13
Milestone: VT Milestone 17: Substantially completed Safeguard Procedure Report Submitted to IRS	6/25/13
Milestone: VT Milestone 9: System Test Complete - Results Submitted to CMS	7/22/13
Group 4	
Milestone: VT Milestone 14: Production Environment Setup Complete	8/15/13
Milestone: VT Milestone 13: Production Testing of Federal Hub Services Complete	8/12/13
Milestone: VT Milestone 15: End to End Testing Complete	8/12/13
Milestone: VT Milestone 16: Test Summary of CMS Test Scenarios Complete	8/22/13
Milestone: VT Milestone 18: Call Center Live	9/16/13
Milestone: VT Milestone 19: Website Launched	9/16/13

Vermont HIX

5.2.9.2 Milestone Payment Schedule

Milestone	Due Date	Milestone Group Total	Payment Schedule	Payment Amount
Group 1		**$ 2,570,901.00**	2/1/2013	$ 848,397.00
Milestone: VT Milestone 4: PM Exchange Components Functional Verification Complete	4/5/13		3/1/2013	848,397.00
Milestone: VT Milestone 2: E&E Exchange Components Functional Verification Complete	4/5/13		4/5/2013	874,105.00
Milestone: VT Milestone 3: FM Exchange Components Functional Verification Complete	4/5/13			**$ 2,570,899.00**
Milestone: VT Milestone 4: Consumer Assistance Functional Verification Complete	4/5/13			
Group 2		**$ 10,604,965.00**	5/1/2013	$ 5,302,483.00
Milestone: VT Milestone 5: Initial PM Exchange Components Development Complete	6/3/13		6/1/2013	5,302,482.00
Milestone: VT Milestone 6: Initial FM Development Complete	6/3/13			**$ 10,604,965.00**
Milestone: VT Milestone 7: Initial E&E Development Complete	6/3/13			
Milestone: VT Milestone 8: Initial CA Development Complete	6/3/13			
Milestone: VT Milestone 10: Connectivity Established for CMS Federal Hub Servics	6/3/2013			
Milestone: VT Milestone 11: Hub Service and partner testing Complete	6/3/13			
Group 3		**$ 8,034,065.00**	7/1/2013	$ 4,017,033.00
Milestone: VT Milestone 12: Communications and Security Testing of Federal Hub Services Review Complete	6/14/13		7/1/2013	4,017,033.00
Milestone: VT Milestone 17: Substantially completed Safeguard Procedure Report Submitted to IRS	6/25/13			**$ 8,034,066.00**
Milestone: VT Milestone 9: System Test Complete - Results Submitted to CMS	7/22/13			
Group 4		**$ 10,926,328.00**	9/1/21013	$ 3,605,688.00
Milestone: VT Milestone 14: Production Environment Setup Complete	8/15/13		10/1/2013	3,605,688.00
Milestone: VT Milestone 13: Production Testing of Federal Hub Services Complete	8/12/13		11/7/2013	3,714,952.00
Milestone: VT Milestone 15: End to End Testing Complete	8/12/13			**$ 10,926,328.00**
Milestone: VT Milestone 16: Test Summary of CMS Test Scenarios Complete	8/22/13			
Milestone: VT Milestone 18: Call Center Live	9/16/13			
Milestone: VT Milestone 19: Website Launched	9/16/13			

Vermont HIX

5.2.9.3 Monthly Payment Sched

Monthly Payments During DDI	Payment Schedule		Payment Amount
Usage of the GSA Cloud during DDI		$	155,088.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,732.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	3/1/13	**$**	**872,473.00**
Usage of the GSA Cloud during DDI		$	155,088.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,732.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	4/5/13	**$**	**872,473.00**
Usage of the GSA Cloud during DDI		$	155,088.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,732.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	5/1/13	**$**	**872,473.00**
Usage of the GSA Cloud during DDI		$	155,088.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,732.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	6/1/13	**$**	**872,473.00**
Usage of the GSA Cloud during DDI		$	155,088.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,732.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	7/1/13	**$**	**872,473.00**
Usage of the GSA Cloud during DDI		$	155,088.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,732.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	8/1/13	**$**	**872,473.00**
Usage of the GSA Cloud during DDI		$	155,088.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,732.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	9/1/13	**$**	**872,473.00**
Usage of the GSA Cloud during DDI		$	155,084.00
Full Implementation of the Dedicated Vblock Hosting Environment			535,733.00
Software Maintenance through DDI (before commencement of M&O)			181,653.00
	11/7/13	**$**	**872,470.00**

Full Implementation of the Hosting Environment	**$**	**1,240,700.00**
Full Implementation of the Dedicated Vblock Hosting Environment	**$**	**4,285,857.00**
Software Maintenance through DDI (before commencement of M&O)	**$**	**1,453,224.00**

Vermont HIX

5.2.9.4 License Payment Schedule

Product	Vendor	Comments	License Type	License Cost[1]
OneGate	Exeter		Enterprise	5,764,706.00
HP Quality Center	HP	- Requirements Management - Defect tracking - Central console for test activity management, execution, and reporting - Supports both manual and automated test approaches (including unit testing, functional testing, regression testing, and performance testing)	30 Concurrent Users	124,712.00
QTP	HP	Testing	3 Concurrent Users	31,178.00
LoadRunner	HP	Load and Performance Testing	1000 Virtual Users	89,723.00
Web Inspect	HP	Security Vulnerability Testing Tools	1 Concurrent User License	31,935.00
JIRA	Atlassian	- Issue and Defect Mgmt	Enterprise 2000 Users	18,476.00
GreenHopper (JIRA Studio)	Atlassian	Features/Task Management	Enterprise 2000 Users	4,619.00
Ensemble	CGI	Internal (CGI) document repository (Issue, Change, Risk, Collaboration, Doc Repository)		19,037.00
CGI SWAT	CGI	Agile tool, sprint management		-
SpringSource	Vmware	Java IDE	Open Source	-
Toad	Quest	DBA Utility; 2 optimizer + 5 standard	2 Optimizer, 5 Standard	13,360.00
Subversion	FOSS/Apache	Version Control	Open Source	-
Maven	FOSS/Apache	Build Tool	Open Source	-
Jenkins/Hudson	FOSS/MIT	Continuous Integration Server	Open Source	-
SONAR	FOSS/LGGPL	Coding Standards (JAVA) (Code Quality Metrics)	Open Source	-
FindBugs	FOSS/LGGPL	Coding Standards (JAVA)	Open Source	-
Checkstyle	FOSS/LGGPL	Coding Standards (JAVA)	Open Source	-
JavaNCSS	FOSS/GGPL	Code Metrics (Java)	Open Source	-
Cobertura	FOSS/GGPL	Code Coverage (Java)	Open Source	-
Javadoc	Oracle	Documentation (Java)	Open Source	-
Junit	FOSS/CPL	Unit Testing tool	Open Source	-
jProfiler	ej technologies	Java Code Profiling	One Server	4,925.00
CA Erwin	CA	Database Design and Data Modeling; 2 workgroup + 5 navigators	2 workgroup, 5 Navigators	15,829.00
Justinmind Prototyper	justinmind.com	Wireframe development	2 User Licenses	1,155.00
XML Spy	Altova	XML Editing Tool	Enterprise	1,154.00
Loqate Verify (Address Verification for USA)	Loqate	Address locations for Oracle Enterprise Data Quality Address Verification Server	1 Server	3,464.00
Liferay Enterprise Edition	FOSS/LGPL	6 Servers 8 cores	2-Production, 5-Non-Production, 2-DR	137,414.00
JAWS	Freedom Scientific	- ADA Compliance verification - Usability Testing	1 License	1,264.00
Thunderhead NOW	Thunderhead	Simple Correspondence	200K-300K	214,348.00
Selenium	FOSS/Apache	Web application record/playback tool used for regression testing of the user interface	Open Source	-
soapUI Pro	soapui.org	Web services test tool; supports automation of web services inspection, invocation, simulation, mockup, functional, load, and compliance tests	10 Licenses	11,618.00
Java PDF417, QR Code Generator	KeepAutomatio		Corporate	3,694.00
Quartz	FOSS/Apache		Open Source	-
SLF4J	FOSS/MIT		Open Source	-
Splunk	splunk.com		500 megabyte-per-day perpetual license plus First Year Support	6,928.00
MagicDraw	magicdraw.com	UML Modeling	5 Users	4,401.00
Eclipse	eclipse.org	Java IDE	Open Source	-
AccVerify	HiSoftware	508 Compliance Check	2 User License for 2 Years	3,169.00
CSSAnalyzer		Usability Testing Tools	Open Source	-
Google Analytics	Google	Web Analytics	Free	-

[1] *Licenses to be paid upon installation*

Configuration Total $ 6,507,109.00

5.2.9.5 M&O Payment Schedule

Line #	Exchange Component	Fixed Costs for Period
1	M&O Base Contract Year 1 (10/1/13 - 9/30/14)[1]:	
	Fixed Software Maintenance	$1,457,282.00
	Fixed Operation Cost	$6,717,260.00
2	M&O Base Contract Year 2 (10/1/14 - 12/31/14)[2]:	
	Fixed Software Maintenance	$365,365.00
	Fixed Operation Cost	$1,666,120.00
3	M&O Optional Contract Year 1 (1/1/15 - 12/31/15)[1]:	
	Fixed Software Maintenance	$1,062,537.00
	Fixed Operation Cost	$6,193,780.00
4	M&O Optional Contract Year 2 (1/1/16 - 12/31/16)[1]:	
	Fixed Software Maintenance	$1,066,873.00
	Fixed Operation Cost	$5,459,050.00

[1] *For Lines 1, 3 and 4 the yearly amount for Fixed Software Maintenance and the Fixed Operations Cost will be invoiced monthly in arrears at 1/12 of the yearly amount.*

[2] *For Line 2 the amount for Fixed Software Maintenance and the Fixed Operations Cost will be invoiced monthly in arrears at 1/3 of the amount for the period.*

5.2.9.6 Payment Schedule Summary

Payment Schedule Summary

Milestone Payment Schedule		
Group 1 Total	$	2,570,899.00
Group 2 Total		10,604,965.00
Group 3 Total		8,034,066.00
Group 4 Total		10,926,328.00
Monthly Payment Schedule		
Full Implementation of the Hosting Environment		1,240,700.00
Full Implementation of the Dedicated Vblock Hosting Environment		4,285,857.00
Software Maintenance through DDI (before commencement of M&O)		1,453,224.00
License Payment Schedule		
Configuration Total		6,507,109.00
M&O Payment Schedule		
Contract Base Year 1 Total		8,174,542.00
Contract Base Year 2 Total		2,031,485.00
Optional Contract Year 1		7,256,317.00
Optional Contract Year 2		6,525,923.00
Grand Total of Payments (Base + Option Years)	**$**	**69,611,415.00**

Amended and Restated Statement of Work No. 1

This Amended and Restated Statement of Work Number 1 ("**Statement of Work**" or "**SOW**") is issued pursuant to the Master Services Agreement first dated as of December 13, 2012, as amended February 28, 2013 (the "**MSA**") between State of Vermont ("**SOV**") and CGI Technologies and Solutions Inc. ("**Supplier**"). This Statement of Work incorporates the terms and conditions of the MSA as if the MSA were fully set forth in the text of this Statement of Work. Capitalized terms not defined in this Statement of Work are defined in the MSA.

1. EFFECTIVE DATE AND TERM OF THIS STATEMENT OF WORK.

This Statement of Work is effective as of December 17, 2012 ("**Statement of Work Effective Date**") and shall continue through December 31, 2014, which shall constitute the "**Statement of Work Term**". The Statement of Work Term may be extended for up to two (2) one-year periods, at the option of SOV.

2. SERVICES TO BE PERFORMED AND SCHEDULE OF PERFORMANCE.

A. Scope of Services

The Supplier will provide (i) IT Services based on the Functional Requirement Traceability Matrix and the Non-Functional Requirement Traceability Matrix (together the "**RTM**") attached here as Schedule A to this SOW and incorporated herein by reference and the (ii) Hosting Services described in Exhibit I. Additional specificity regarding the scope of Services is provided for in Exhibit E (Scope Assumptions) to the MSA. As described in Section 17 below, the scope of Hosting Services will be further developed and refined by mutual agreement of the parties by March 1, 2013, or such other date mutually agreed by the parties pursuant to a Change Order ("**Revised Hosting Scope Date**").

B. Location of Services.

Supplier will perform Services under this SOW at a SOV provided facility. Supplier will also perform testing services at its facility in Belton, Texas. All Hosting Services will be located in the U.S.

C. Deliverables and Work Product.

CGI will perform or deliver, as applicable, the deliverables as set forth in the MSA, including, without limitation, the deliverables as set forth in Exhibit E and Exhibit L attached to the MSA (including a cost schedule and an executive summary). Additional details regarding the deliverables and work product are documented in the Project Management Plan ("**PMP**").

D. Milestone Schedule

Supplier will provide the Services in accordance with the timeframes set forth in the Baseline Schedule. A list of Critical Milestones subject to liquidated damages is included in Exhibit C.

E. Acceptance Criteria and Process.

The Deliverable acceptance criteria and process is set forth in the PMP.

F. Supplier Personnel.

Process for approval of Supplier Personnel in Key Supplier Positions is described in the MSA and Exhibit E.

G. Supplier Resources.
Description of Supplier Resources will be set forth in the PMP. A list of Supplier Resources is included in Exhibit E (Scope Assumptions).

H. SOV Roles and Responsibilities.
1. Services or Support: See Exhibit E (Scope Assumptions) to the MSA.
2. Facilities, Equipment and SOV Resources: See Exhibit E (Scope Assumptions) to the MSA.
3. Proprietary Materials: SOV will provide licenses for all Oracle products.

I. Governance Structure, Meetings and Reports.
Governance Structure, Operation and Executive level meeting process and weekly status report standards will occur as set forth in the PMP.

J. Termination for Convenience.
Notwithstanding Section 26.3 of the MSA, at any time prior to the date fifteen (15) days after the Revised Hosting Scope Date, SOV shall have the right to terminate this Statement of Work, in whole or in part, for convenience and without cause by providing Supplier with not less than fifteen (15) days prior written notice. Upon any such termination, SOV shall have no liability other than to (i) pay Supplier Charges for Services rendered up to and including the effective date of termination; and (ii) reimburse Supplier for Pass-Through Expenses incurred by Supplier to procure Software or Hardware for SOV pursuant to Section 6 and 7 below, or as approved by SOV pursuant to a Change Order. In the event of a termination in part, Charges will be adjusted in accordance with Section 26.4.

---

3. HOSTING SERVICES.
See Exhibit I (Hosting Services) to the MSA

---

4. PROJECT MANAGERS.
See Exhibit E (Scope Assumptions) to the MSA.

---

5. STAFF.
A. Subcontractors.

Supplier expects to engage Exeter Consulting (and its affiliates) to configure the OneGate product. The scope of the subcontractor configuration work is set forth in the PMP and the RTM.

---

6. SOFTWARE.

A. Third Party Software provided by Supplier

Subject to the terms and conditions of the MSA, Supplier will procure the following Third Party Software for SOV (the licenses for which will be directly between Supplier and the respective third party vendor):

Liferay

OneGate

Thunderhead

B. Third Party Software provided by SOV.

SOV will provide licenses for Oracle products and will pay maintenance on those products during the term of the SOW.

---

7. HARDWARE.

Not applicable at this time

---

8. THIRD PARTY CONTRACTS.

NONE AT THIS TIME.

---

9. SERVICE LEVELS.

See Exhibit D attached to the MSA.

---

10. SECURITY, DISASTER RECOVERY, BUSINESS CONTINUITY PROCEDURES, CONTROLS

See MSA and Exhibit D (Service Levels) and Exhibit J (Supplier Contingency Plans) attached to the MSA.

---

11. FORECASTING

Any forecasting needed is as set forth in in the PMP.

---

12. FACILITIES TO BE PROVIDED BY SUPPLIER.

Not applicable.

---

13. ASSUMPTIONS.

A. See Exhibit E (Scope Assumptions) attached to the MSA.

14. OPTIONAL SERVICES.

A. Not applicable to this SOW.

15. OTHER SERVICES.

A. Not applicable to this SOW

16. CHARGES AND PASS-THROUGH EXPENSES.

A. See Exhibit L (Cost) attached to the MSA.

17. ADDITIONAL TERMS.

The parties agree to negotiate in good faith during the period prior to the Revised Hosting Scope Date to agree to the scope of the hosting services set forth in Exhibit I. This SOW, Exhibit D, Exhibit I, Exhibit L and, as necessary, other related documents will be revised (either by means of an amendment to the MSA or by Change Order as appropriate) to reflect the mutually agreed terms by the Revised Hosting Scope Date.

Agreed to and accepted by:

CGI Technologies and Solutions Inc. (CGI)	State of Vermont
By: E-SIGNed by Gregg Mossburg on 2013-Mar-01	By: E-SIGNed by Mark Larson on 2013-Mar-01
Name:	Name:
Title:	Title:
Date:	Date:

SCHEDULE A

RTM

[see attached]

Appendix B: Business and Technical Requirements and Bidder Response Matrix

Instructions for completing the Requirements Response Matrix

Bidders are required to provide a response, using the appropriate codes provided in the table below, for each requirements listed in each of the four (4) tabs included in this Requirements Response Matrix

--Individual Eligibility Requirements
--Individual Enrollment Requirements
--Plan Management Requirements
--SHOP Requirements
--Financial Management Requirements
--Administrative Requirements
--Reporting Requirements
--Noticing Requirements
--Technical Requirements
--Web Portal UX Requirements
--Consumer Assistance - General Requirements
--Consumer Asssitance - Case Management Requirements
--Consumer Assistance - Navigator Requirements

Bidders must provide, for each requirement listed, the corresponding Proposal section reference explaining the bidder's response.

The matrix also provides a column where Bidders may provide additional comments/clarifications related to a specific requirements response

Code	Condition	Description
S	Standard Function	The proposed system fully satisfies the requirement as stated. The vendor must explain how the requirement is satisfied by the system.
W	Workflow or System Configuration Required	Current functionality of the proposed system exists in the system and can be modified by a system administrator to meet this requirement.
M	Modification Required	The proposed system requires a modification to existing functionality to meet this requirement which requires a source code modification. The system will be modified to satisfy the requirements as stated or in a different format. The vendor must explain the modifications and include the cost of all modifications above and beyond the base cost in the ***Project Cost Proposal***.
F	Planned for Future Release	This functionality is planned for a future release. The vendor must explain how the requirement will be satisfied by the system and when the release will be available.
C	Custom Design and Development	The proposed system requires new functionality to meet this requirement which requires a source code addition. The vendor must explain the feature and its value, and include any cost above and beyond the base cost in the ***Project Cost Proposal***.
N	Cannot Meet Requirement	The proposed system will not satisfy the requirement. The vendor must explain why the requirement cannot be satisfied.
O	Other Software	If the requirement is to be satisfied through the use of a separate software package(s), vendors must identify those package(s) and describe how the functionality is integrated into the base system.

Individual Eligibility Requirements Traceability Matrix

EL-1	Eligibility and Enrollment	General	OneGate/Oracle Identity Manager	OneGate/Oracle Identity Manager	Provide role-based access control to allow users to perform certain operations assigned to specific roles (e.g., Exchange Staff, Individuals, Brokers, and Navigators).	S	
EL-2	Eligibility and Enrollment	Pre-Screening	OneGate	OneGate	Interface with the DHS Eligibility System to provide Individuals and authorized representatives with the option to complete pre-screening for eligibility for State health plans through a real-time interface with the DHS Eligibility System with the option for anonymous screening.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
EL-3	Eligibility and Enrollment	Pre-Screening	OneGate	OneGate	Interface with the DHS Eligibility System to provide Individuals and authorized representatives with the option to complete pre-screening for eligibility for State health plans through a real-time interface with the Federal Exchange Eligibility Service with the option for anonymous screening.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
EL-4	Eligibility and Enrollment	Pre-Screening	N/A	N/A	Interface with the DHS Eligibility System to provide an expert-level pre-screening function to Navigators, Brokers, and Exchange Staff.	N/A	*1/4/2013 - this will be included in the requirements for VT*

Individual Eligibility Requirements Traceability Matrix

EL-5	Eligibility and Enrollment	Pre-Screening	OneGate	OneGate	Indicate whether an applicant is already enrolled in a publicly subsidized health coverage program.	W	
EL-6	Eligibility and Enrollment	Pre-Screening	OneGate	OneGate	Present a more detailed level of screening questions to be addressed at the option of the Individual.	S	
EL-7	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Interface with the DHS Eligibility System to display eligibility information for VT subsidized public and commercial health plans available through the Exchange.	C	Interfacing with other systems (such as the Federal Eligibility Data Hub and State data sources) should be completed during appropriate stages in the application process. Other than the verification of residence and citizenship and immigration
EL-8	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Interface with the DHS Eligibility System to display eligibility information and supporting data for the Advance Premium Tax Credits and Cost Sharing Reductions.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.

Individual Eligibility Requirements Traceability Matrix

EL-9	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Interface with the Federal Exchange Eligibility Servce to display eligibility information and supporting data for the Advance Premium Tax Credits and Cost Sharing Reductions.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
EL-10	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Process the Advance Premium Tax Credit and Cost Sharing Reduction amount(s) provided by CMS/IRS and update the individual's account.	W	
EL-11	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide Individuals with the option to accept a lower Advance Premium Tax Credit.	S	
EL-12	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Allow Exchange Staff, Individuals, Brokers, and Navigators to view alerts regarding the need to recalculate the tax credit when needed.	W	

Individual Eligibility Requirements Traceability Matrix

EL-13	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide the capability for an Individual to identify the source of information used to determine eligibility.	W	
EL-14	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide individuals with the ability to acknowledge an eligibility determination.	S	
EL-15	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Allow Exchange Staff to submit case information for eligibility determination outside of the standard workflow.	S	
EL-16	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Send real-time, automated notifications and written notices to Individuals of CMS determinations of exemption status, and update individual accounts accordingly.	W	

Individual Eligibility Requirements Traceability Matrix

EL-17	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide the ability to generate online and written notification of the result of an Individual's eligibility determination, including the basis for denial if denied coverage.	S	
EL-18	Eligibility and Enrollment	Individual Application & Submit Update	N/A	N/A	Provide electronic notification to CMS of the result of an Individual's eligibility determination.	N/A	In accordance with RFP Amendment 2 Question 200 this requirement is deleted. *1/04 - Related to the differentiation of responsibilities. Revisit for VT.*
EL-19	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Send notifications to the Individuals, alerting them to submit required eligibility or verification information.	S	
EL-20	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Send notifications to the Individuals who have not completed their applications informing them of the expiration date.	W	

Individual Eligibility Requirements Traceability Matrix

EL-21	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Send notifications to the Individuals, Exchange Staff, Brokers, and Navigators of changes to Individuals' applications.	W	
EL-22	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Send notifications to the Individuals regarding the enrollment process and the status of their application.	S	
EL-23	Eligibility and Enrollment	Individual Application & Submit Update	Oracle Identity Management	Oracle Identity Management	Determine if users requesting new access already have system access, assist known Individuals in recovering login information, and assist new Individuals in setting up access	S	
EL-24	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide for the management of the Individual's application intake process, including viewing, updating and displaying the Individual's and household's eligibility history to authorized users.	S	

Individual Eligibility Requirements Traceability Matrix

EL-25	Eligibility and Enrollment	Individual Application & Submit Update	Oracle MDM (Customer Hub)	Oracle MDM (Customer Hub)	Use a single Exchange-specified client identifier for all solution functions and interfaces, and provide cross-referencing to other system identifiers where required.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
EL-26	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide a consolidated online application for all programs offered through the Exchange, including but not limited to Medicaid, other VT public health and human service programs, and commercial health insurance subsidies.	W	*Choosing to use the Federal single application for insurance affordability programs (approved by the Secretary)*
EL-27	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Intake applicant information, including attachments, required to determine eligibility for publically subsidized health coverage programs offered through the Exchange.	S	
EL-28	Eligibility and Enrollment	Individual Application & Submit Update	N/A	N/A	Route applicant data, and related attachments, to the DHS Eligibility System to determine real-time eligibility for publically subsidized programs and commercial health coverage programs offered through the Exchange.	N/A	*1/4/2013 - this will be included in the requirements for VT. Does VT want their Eligibility system to make the determination for subsidized program AND non-subsidized programs?*

Individual Eligibility Requirements Traceability Matrix

EL-29	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Route applicant data, and related attachments, to the Federal Exchange Eligibility Service to determine real-time eligibility for publically subsidized programs and commercial health coverage programs offered through the Exchange.	C	out of scope
EL-30	Eligibility and Enrollment	Individual Application & Submit Update	N/A	N/A	Route eligibility related attachments from users to Medicaid/CHIP to support eligibility processing and determination.	N/A	*1/4/2013 - this will be included in the requirements for VT*
EL-31	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide the capability to identify Navigators and Brokers if they are completing applications on behalf of an Individual.	S	
EL-32	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide the capability for the Individual to attest that any information provided by a Navigator or Brokers is accurate.	S	

Individual Eligibility Requirements Traceability Matrix

EL-33	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Allow continuance of the application process for Individuals without an SSN (e.g. newborns and undocumented Individuals).	S	
EL-34	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Display an Individual's eligibility and subsidies under all tiers of QHP benefits through an interface with the DHS Eligibility System.	W	Not clear how the definitive source of the information will occur.
EL-35	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide the capability for an Individual to indicate various types of potential exemptions through the single, integrated application process.	W	For MAGI, there's a limited set of exemptions. For the traditional medicaid and other eligibility programs, there are more financial considerations.
EL-36	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Process documents received in the mail, via facsimile, web portal, and/or email.	S	

Individual Eligibility Requirements Traceability Matrix

EL-37	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Allow qualified Native Americans to switch plans on a monthly basis.	W	Based on meeting on 12/19, this to be provided as the mandate is at the Federal level. No VT tribes but recognize indviduals in VT may be associated with a qualitifed Native American tribe.
EL-38	Eligibility and Enrollment	Individual Application & Submit Update	N/A	N/A	Provide the capability to eliminate all cost-sharing for Native Americans enrolled in any QHP through the Exchange whose household income is less that 300 percent FPL.	N/A	Based on meeting on 12/19, this to be provided as the mandate is at the Federal level. No VT tribes but recognize indviduals in VT may be associated with a qualitifed Native American tribe.
EL-39	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Allow for the indication / determination of an applicant's membership in a Native American tribe, as defined by the ACA as well as Medicaid.	W	because of ACA and MAGI regulations that consider Native American within the eligibility, leave in for the time being and revisit
EL-40	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Provide the capability to adjust the calculation of MAGI with allowed exclusions for qualified Native Americans per the ACA regulations.	W	because of ACA and MAGI regulations that consider Native American within the eligibility, leave in for the time being and revisit

Individual Eligibility Requirements Traceability Matrix

EL-41	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	OneGate	Distribute and collect, through a range of mediums, individual, employer, and employee enrollment forms.	W	
EL-42	Eligibility and Enrollment	Individual Application & Submit Update	N/A	N/A	Provide an indicator for individuals determined eligible for Medicaid and CHIP who access coverage through the Exchange	N/A	out of scope
EL-43	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Ask knowledge-based ID questions based on data gathered from external data sources to facilitate authentication of identity.	W	
EL-44	Eligibility and Enrollment	Individual Eligibility Determination-Verification	Oracle Identity Management	Oracle Identity Management	The solution may request proof of identity from Individuals, Brokers, and Navigators (driver's license, passport) if a higher level of trust is required.	W	

Individual Eligibility Requirements Traceability Matrix

EL-45	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Validate Individual application information for completeness of data and prompt the Individual for additional information, if applicable.	S	
EL-46	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide the capability to gather and display Individual and household eligibility data from external sources.	W	
EL-47	Eligibility and Enrollment	Individual Eligibility Determination-Verification	Loqate	Loqate	Validate mailing addresses provided in applications (using an external Postal Address validation service).	S	
EL-48	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Allow for a manual verification process when the federal hub verification service is not available through the business rules engine.	S	

Individual Eligibility Requirements Traceability Matrix

EL-49	Eligibility and Enrollment	Individual Eligibility Determination-Verification	Siebel Public Sector CRM	Siebel Public Sector CRM	Support a dispute process.	W	
EL-50	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide capability to manually update incarceration status based documentation provided by the Individual (e.g. release papers).	W	Is this a MAGI factor within VT - incarceration may / may not impact residence requirements?
EL-51	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Produce an immediate on-screen notification of a positive incarceration data match, and allow the Individual of ability to provide alternate documentation or an attestation of incarceration status.	W	Is this a MAGI factor within VT - incarceration may / may not impact residence requirements?
EL-52	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Update individual accounts with the verification results as appropriate.	S	*1/4 - Hawaii didn't provide any additional information. There may be additional verification options/needs than those identified in the other requrements.*

Individual Eligibility Requirements Traceability Matrix

EL-49	Eligibility and Enrollment	Individual Eligibility Determination-Verification	Siebel Public Sector CRM	Siebel Public Sector CRM	Support a dispute process.	W	
EL-50	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide capability to manually update incarceration status based documentation provided by the Individual (e.g. release papers).	W	Is this a MAGI factor within VT - incarceration may / may not impact residence requirements?
EL-51	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Produce an immediate on-screen notification of a positive incarceration data match, and allow the Individual of ability to provide alternate documentation or an attestation of incarceration status.	W	Is this a MAGI factor within VT - incarceration may / may not impact residence requirements?
EL-52	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Update individual accounts with the verification results as appropriate.	S	*1/4 - Hawaii didn't provide any additional information. There may be additional verification options/needs than those identified in the other requrements.*

Individual Eligibility Requirements Traceability Matrix

EL-57	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Allow Exchange Staff, Brokers, and Navigators to view, save, and print Individual verification documents that have been up-loaded to a case.	S	
EL-58	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide the capability to allow designated users to confirm, notate and mark active/non-active status of verification documents and verification results.	S	
EL-59	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Allow Exchange Staff, Individuals, Brokers, and Navigators to provide alternative verification through multiple methods.	S	
EL-60	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide the ability to allow Individuals to view, confirm, dispute and submit corrections to verification results.	W	

Individual Eligibility Requirements Traceability Matrix

EL-61	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Support checks for Medicaid eligibility that can not be serviced real-time. Responses shoould be accepted later, and user shall be permitted to negotiate enrollment in a QHP while waiting for a response.	M	CGI Team will modify the Siebel workflow to support this requirement.
EL-62	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide the capability to accept notifications from Medicaid/CHIP regarding loss of coverage, and should evaluate those individuals for QHP subsidized coverage.	F	Capability will be available in April 2013 in OneGate
EL-63	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide individuals the ability to have a reasonable opportunity (90-day period under PPACA) to address inconsistencies reported by external entities (i.e. income, citizenship, etc.)	F	Capability will be available in April 2013 in OneGate
EL-64	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	OneGate	Provide the capability for an Individual to indicate or attest to affiliation with recognized Native American tribe during the application process, request verification and update the individual account with verified information.	F	out of scope

Individual Eligibility Requirements Traceability Matrix

EL-65	Eligibility and Enrollment	Change Management	N/A	N/A	Provide the ability to update information related to other components of eligibility not described above, including access to minimum essential coverage.	N/A	out of scope
EL-66	Eligibility and Enrollment	Change Management	OneGate	OneGate	Reassess and determine eligibility based on the new circumstances. For every data field, the system must be configurable to force an eligibility determination/re-determination based on revised data input.	W	
EL-67	Eligibility and Enrollment	Change Management	OneGate	OneGate	Provide consumers the ability to view the new determination of eligibility after the change in circumstances.	S	
EL-68	Eligibility and Enrollment	Change Management	OneGate	OneGate	Provide users the ability to choose new health plans after the re- determination process based on the new circumstances.	S	

Individual Eligibility Requirements Traceability Matrix

EL-69	Eligibility and Enrollment	Case Inquiry	OneGate	OneGate	Allow Exchange Staff, customers, call center staff and Navigators to search for a customer's household information and composition.	W	
EL-70	Eligibility and Enrollment	Case Inquiry	OneGate	OneGate	Allow Exchange Staff, customers, call center staff and Navigators to view a customer's household information and composition.	S	
EL-71	Eligibility and Enrollment	Case Inquiry	OneGate	OneGate	Allow Exchange Staff, customers, call center staff and Navigators to add, update, modify and delete household composition information.	S	
EL-72	Eligibility and Enrollment	Identify Management	Oracle MDM (Customer Hub)	Oracle MDM (Customer Hub)	Provide automatic checks for duplicate household members within other cases in the system.	W	

Individual Eligibility Requirements Traceability Matrix

EL-73	Eligibility and Enrollment	Identify Management	OneGate	OneGate	Allow Exchange Staff, call center staff and Navigators to merge or associate different household members together.	W	
EL-74	Eligibility and Enrollment	Identify Management	OneGate	OneGate	Provide the ability to split family relationships and to assign certain field information to the appropriate people.	W	

Individual Eligibility Requirements Traceability Matrix

ELM-1	Eligibility and Enrollment	Pre-Screening	**OneGate**	Provide the option for anonymous completion of MAGI eligibility related questions	S	
ELM-2	Eligibility and Enrollment	Pre-Screening	OneGate	The following MAGI related data items should be requested in the pre-screening: financial, residency, person specific (age, gender, pregnant, disability, tribal affiliation) relationships to other household members	S	
ELM-3	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide a more detailed / specific application to be completed for MAGI MAGI QHP eligibility (incl. APTC, CSR).	S	
ELM-4	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	As part of the application process, collect State residence information in accordance with the Federal and State regulations and necessary to establish MAGI QHP eligibility (incl. APTC, CSR).	S	

Individual Eligibility Requirements Traceability Matrix

ELM-5	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	As part of the application process, collect citizenship / immigration status information as necessary to establish MAGI QHP eligibility (incl. APTC, CSR).	S	
ELM-6	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	As part of the application process, collect household and income information to determine if the household is under 100% FPL.		
ELM-7	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	As part of the application process, support collecting additional household information and income information as necessary to establish MAGI QHP eligibility (incl. APTC, CSR).	S	IRS and other sources.

Individual Eligibility Requirements Traceability Matrix

ELM-8	Eligibility and Enrollment	Change Management	OneGate	Store changed information along with the date the information was changed.	S	
ELM-9	Eligibility and Enrollment	Change Management	OneGate	Support prompting users / consumers to renew their application on an annual basis.	S	
ELM-10	Eligibility and Enrollment	General	OneGate	Allow business users, as determined by the State, to easily read / modify the eligibility determination rules with minimal IT support.	S	OPA capability
ELM-11	Eligibility and Enrollment	Program Policy	OneGate	Provide a method to identify persons who are eligible for services.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-12	Eligibility and Enrollment	Program Policy	CGI Solution	Be scalable and flexible enough to accommodate and adapt to changes required by State and/or Federal statute, regulation, mandate, decision, or policy.	S	
ELM-13	Eligibility and Enrollment	Program Policy	OneGate	Allow individuals in a household to be eligible under different categories and receive different benefits related to MAGI QHP/APTC/CSR based upon individual information.	S	
ELM-14	Eligibility and Enrollment	Application Process	OneGate	Provide an [anonymous] screening tool that is compatible with the HBE and allows an applicant to answer an initial basic set of questions to quickly identify potential eligibility for MAGI QHP (incl. APTC, CSR).		
ELM-15	Eligibility and Enrollment	Application Process	OneGate	Provide customized local office information, through public-facing front-end (i.e. physical location of nearest local office and name, email and phone number).	M	

Individual Eligibility Requirements Traceability Matrix

ELM-16	Eligibility and Enrollment	Application Process	OneGate	Provide interactive questions that can lead to appropriate next questions, to include identification of an ABD-applicant, in need for a supplemental form(s), based on responses and other existing data necessary to establish MAGI QHP eligibility (incl. APTC, CSR). .		
ELM-17	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to define required and optional fields, including default data values as applicable, based on the MAGI QHP eligibility (incl. APTC, CSR). program rules.	S	
ELM-18	Eligibility and Enrollment	Application Process	OneGate	Identify and display verifications required for the applicant based on program rules.	S	
ELM-19	Eligibility and Enrollment	Application Process	OneGate	Produce a customized listing of verification documents for an eligibility criteria required to complete eligibility determination.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-20	Eligibility and Enrollment	Application Process	OneGate	Allow the worker/applicant to upload and attach source documents to support eligibility determination.	S	
ELM-21	Eligibility and Enrollment	Application Process	OneGate	Present the applicant with a summary view of the information entered prior to submission.	S	
ELM-22	Eligibility and Enrollment	Application Process	OneGate	Allow applicants to print /save a copy of electronic copy for their records.	S	
ELM-23	Eligibility and Enrollment	Application Process	OneGate	Allow an applicant or applicant's authorized representative to review the current application before and after formal submission.		

Individual Eligibility Requirements Traceability Matrix

ELM-24	Eligibility and Enrollment	Application Process	OneGate	Allow an applicant or applicant's representative to amend an application as long as a determination has not been made.	S	
ELM-25	Eligibility and Enrollment	Application Process	OneGate	Allow the applicant or applicant's authorized representative to save and amend the application or renewal for up to 30 days in order to gather additional information prior to submittal.	S	
ELM-26	Eligibility and Enrollment	Application Process	OneGate	Allow and record an applicant's request to withdraw an application.	F	
ELM-27	Eligibility and Enrollment	Application Process	CGI	Collect and manage information about beneficiary population from diverse sources.		

Individual Eligibility Requirements Traceability Matrix

ELM-28	Eligibility and Enrollment	Application Process	OneGate	Provide an automated or guided application process to enable the applicant/worker to easily enter required information.	S	
ELM-29	Eligibility and Enrollment	Application Process	OneGate	Provide system-generated date and time stamp for receipt of electronic applications to be used in monitoring standards of promptness by program.	S	
ELM-30	Eligibility and Enrollment	Application Process	CGI	Provide system-generated date and time stamp for registration of paper applications.		
ELM-31	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to begin benefits on a date different than the application date and system-generated date.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-32	Eligibility and Enrollment	Application Process	OneGate	Capture and display date that a disposition was made on an application/renewal.	S	
ELM-33	Eligibility and Enrollment	Application Process	OneGate	Provide the capability for an applicant to indicate various types of potential exemptions through the single, integrated application process.	S	
ELM-34	Eligibility and Enrollment	Application Process	OneGate	Route applications to the appropriate staff, based on business rules.	W	
ELM-35	Eligibility and Enrollment	Application Process		Display to the applicant discrepant information between the new application and information stored in the existing household.		

Individual Eligibility Requirements Traceability Matrix

ELM-36	Eligibility and Enrollment	Application Process	OneGate	Allow for a manual verification process when the Federal or State hub verification service is not available.	W	
ELM-37	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to indicate which verification documents have already been provided.	S	
ELM-38	Eligibility and Enrollment	Application Process	CGI	Provide applicants the ability to submit alternative verification via multiple avenues (e.g., email, mail, phone, fax, walk- in).		
ELM-39	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to manually extend verification timeframes.	W	

Individual Eligibility Requirements Traceability Matrix

ELM-40	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to track required verification timeframes.	W	
ELM-41	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to generate a list of received and pending verifications including eligibility worker entered comments.	W	
ELM-42	Eligibility and Enrollment	Application Process	OneGate	Provide the ability to allow applicants to view, confirm, dispute and submit corrections to verification results.	W/F	
ELM-43	Eligibility and Enrollment	Application Process	OneGate	Provide applicants the ability to address inconsistencies reported by external entities (i.e. income, citizenship, etc.) within a timeframe defined by the State.	W	

Individual Eligibility Requirements Traceability Matrix

ELM-44	Eligibility and Enrollment	Application Process	OneGate	Update the applicant's record with the verification results as appropriate.	W	
ELM-45	Eligibility and Enrollment	Application Process	OneGate	Assure consistency in eligibility determination processing when applicants attempt to access services through different entry points.	S	
ELM-46	Eligibility and Enrollment	Application Process	OneGate	Provide the capability to determine and correct eligibility for current and prior months.	W	
ELM-47	Eligibility and Enrollment	Application Process	OneGate	Display the eligibility results in a manner that is comprehensive and easy to understand.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-48	Eligibility and Enrollment	Household Maintenance	OneGate	Provide the capability to create and maintain an electronic household file of all applicants and families requesting MAGI QHP/APTC/CSR from the time that they first make an entry to the system.		
ELM-49	Eligibility and Enrollment	Household Maintenance	tbd	Auto-populate known data within the system between modules and functions within the life of the household.		
ELM-50	Eligibility and Enrollment	Household Maintenance	tbd	Provide a mechanism to edit and store certain automatically populated data as defined by the State.		
ELM-51	Eligibility and Enrollment	Household Maintenance	OneGate	Allow authorized users to search online household files using key fields such as name, SSN, ID, date of birth, etc.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-52	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism for authorized users to access beneficiary/household summary from any screen.	M	
ELM-53	Eligibility and Enrollment	Household Maintenance	OneGate	Provide the functionality to reinstate service coverage until the Administrative Appeals decision is rendered.	W	
ELM-54	Eligibility and Enrollment	Household Maintenance	OneGate	Provide the capability at an individual level to be able to rework a prior involvement that is closed even if an open involvement exists.	W/M	
ELM-55	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism to indicate relationships between all members of a household.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-56	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism to automatically create the inverse family relationships (e.g., parent – child, child – parent, etc.).	S	
ELM-57	Eligibility and Enrollment	Household Maintenance	CGI	Provide the capability to perform mass terminations due to changes in status as well as program changes.		
ELM-58	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism to indicate that a beneficiary/household is under review.	W	
ELM-59	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism to alert management that pending applications have exceeded specified time limits.	W	

Individual Eligibility Requirements Traceability Matrix

ELM-60	Eligibility and Enrollment	Household Maintenance	OneGate	Automatically create an alert of approaching deadlines.	W	
ELM-61	Eligibility and Enrollment	Household Maintenance	OneGate	Allow applicant/beneficiaries to self-report changes in their personal information online, notify the appropriate eligibility worker based on parameters described by the State when changes are made.	W	
ELM-62	Eligibility and Enrollment	Household Maintenance	OneGate	Provide the capability to view the new determination of eligibility after the change in information.	S	
ELM-63	Eligibility and Enrollment	Household Maintenance	OneGate	Automatically close beneficiaries/households/categories based on applicable eligibility rules resulting from changes in information and track closure reasons.	S/W	

Individual Eligibility Requirements Traceability Matrix

ELM-64	Eligibility and Enrollment	Household Maintenance	OneGate	Provide functionality to manually close beneficiaries/households/categories based on applicable eligibility rules resulting from changes in information and track closure reasons.	W	
ELM-65	Eligibility and Enrollment	Household Maintenance	Audit Logging	Provide the capability to track and record any changes to an individual's information.		
ELM-66	Eligibility and Enrollment	Household Maintenance	Audit Logging	Allow authorized users to update, add persons, and relationships to an existing household and maintain a history thereof.		
ELM-67	Eligibility and Enrollment	Household Maintenance	OneGate	Change the status of any individual in a household without terminating eligible household members.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-68	Eligibility and Enrollment	Household Maintenance	OneGate	Provide web-based functionality to allow the applicant to renew eligibility online.	S	
ELM-69	Eligibility and Enrollment	Household Maintenance	CGI	Allow for renewals that do not occur online.		
ELM-70	Eligibility and Enrollment	Household Maintenance	OneGate	Track when a renewal is due.	W	
ELM-71	Eligibility and Enrollment	Household Maintenance	OneGate + CGI noticing	Have the ability to track which renewals have been sent and which have been returned.	W/M	

Individual Eligibility Requirements Traceability Matrix

ELM-72	Eligibility and Enrollment	Household Maintenance	OneGate + CGI noticing	Have the ability to automatically send renewal notices to beneficiaries	W/M	
ELM-73	Eligibility and Enrollment	Household Maintenance	OneGate + CGI noticing	Have the ability to pre-populate renewal forms with beneficiary information that is currently on file and allow the beneficiary to change or add information.	W/M	
ELM-74	Eligibility and Enrollment	Household Maintenance	OneGate	Renew eligibility based on Federal and State statutes and regulations as necessary to establish MAGI QHP eligibility (incl. APTC, CSR).	S	
ELM-75	Eligibility and Enrollment	Household Maintenance	OneGate	Recalculate and redetermine eligibility when a change in circumstance occurs (e.g., household composition changes, child turning 19).	S	

Individual Eligibility Requirements Traceability Matrix

ELM-76	Eligibility and Enrollment	Household Maintenance	OneGate	Track and allow beneficiaries who did not return the pre-populated renewal form or the required documentation and are terminated on that basis a reconsideration period, as defined by the State, when the State would reconsider eligibility without a new application and renew eligibility if necessary information is provided.	W	
ELM-77	Eligibility and Enrollment	Household Maintenance	OneGate	Provide the capability to automate the renewal process if all information remains the same or if verified information remains within applicable limits.	W	
ELM-78	Eligibility and Enrollment	Household Maintenance	OneGate	Assure renewal forms meet the same accessibility standards as application.	S	

Individual Eligibility Requirements Traceability Matrix

ELM-79	Eligibility and Enrollment	Household Maintenance	CGI	Provide the functionality to routinely (e.g., daily, weekly, or monthly as determined by the State) match available data in the State Data Hub or with other interfaces to identify recipient changes (e.g., obtain employment (via DLIR), begin receiving other TPL (via TPL vendor), deceased (via DOH vital statistics), or enter prison (via Public Safety).		
ELM-80	Eligibility and Enrollment	Workflow Management	OneGate	Support both task-based and household-based operations.	W	
ELM-81	Eligibility and Enrollment	Workflow Management	OneGate	Provide the capability to save work in progress, exit the workflow, access work at a later point with all of the information still populated from the previous worker's actions so as previous work will not need to be repeated and the worker can enter the workflow where they left off.	W	
ELM-82	Eligibility and Enrollment	Workflow Management	OneGate	Track, monitor, and display work done/ in queue to supervisors.	W	

Individual Eligibility Requirements Traceability Matrix

ELM-83	Eligibility and Enrollment	Financial Assistance	OneGate	Flag any household record Change of Circumstance so that the eligibility workers can determine the derivation of the Change of Circumstance.	W	
ELM-84	Eligibility and Enrollment	Financial Assistance	OneGate	Flag household record Change of Circumstance and allow DHS to designate changes that will be automatically accepted, pended for review, maintained as notes, rejected or other action.	W	
ELM-85	Eligibility and Enrollment	Interfaces	CGI	Alert eligibility workers or a processing queue when beneficiary information is updated through an automated interface.		
ELM-86	Eligibility and Enrollment	Interfaces	CGI/Oracle	Provide a Business Rules Engine to access two-way, real-time interfaces with existing State databases to verify application data (e.g., State wage data, incarceration data) as required.		

Individual Eligibility Requirements Traceability Matrix

ELM-87	Eligibility and Enrollment	Interfaces	CGI	Provide the ability to leverage the federal approach to verification from federal agencies such as the Internal Revenue Service, Department of Health and Human Services, and Department of Homeland Security to eliminate the independent establishment of those interfaces and connections at the State level.		

Individual Enrollment Requirements Traceability Matrix

EN-1	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Prepare an enrollment questionnaire to gather individual preferences and help refine choices of plan to be displayed.	S	
EN-2	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Store enrollment questionnaire responses and display plan choices based on questionnaire / filtering criteria.	S	
EN-3	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Based on issuer and plan information gathered, display plan cost and availability.	S	
EN-4	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	As a default, only display health plans that have been certified by the exchange, are open to additional enrollment, and are available in the individual's geographic area.	S	

Individual Enrollment Requirements Traceability Matrix

EN-5	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Display actual plan cost based on applicable rating factors (individuals covered, age, geography, etc.) provided by the individual during the application process.	S	
EN-6	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	If applicable, display an adjusted plan cost based on reduced cost sharing or tax credit advance eligibility.	S	
EN-7	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Provide an individual the capability to apply the Tax Credit Advance (if eligible) to his / her monthly premium payment or decline the advance, allowing individuals the ability to alternatively claim tax credits at time of annual income tax filing.	S	
EN-8	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Generate written notification to individuals who select at Tax Credit Advance of the possibility of tax penalties / liabilities at time of tax filing should their annual income increase.	W	

Individual Enrollment Requirements Traceability Matrix

EN-9	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Generate on-screen notification to individuals who select at Tax Credit Advance of the possibility of tax penalties / liabilities at time of tax filing should their annual income increase.	S	
EN-10	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Provide capability to display a detailed comparison of available health plans based on individual preferences.	S	
EN-11	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Provide capability for individuals to adjust individual preferences and update display / comparison of available qualified health plans. This capability includes the ability to further refine or constrain filtering criteria to either display a greater or lesser number of plan choices.	S	
EN-12	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Provide hyperlinks to Issuer/Plan sites for individuals to obtain further information from Issuers	W	

Individual Enrollment Requirements Traceability Matrix

EN-13	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Provide capability for an individual to select a QHP and initiate the enrollment process.	S	
EN-14	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Prevent individuals that have a current QHP selection pending from adding a new QHP or changing their pending selection.	M	OneGate will provide the mechanism to add or modify their QHP selection if it is a pending state.
EN-15	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Once a plan is selected, direct an individual to issuer-specific specific instructions on payment remittance for monthly premiums.	W	
EN-16	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	Update an individuals account to reflect plan selection and the effective plan-year.	S	

Individual Enrollment Requirements Traceability Matrix

EN-17	Eligibility and Enrollment	Plan Selection	Healthation	Premium Processor / One Gate	After plan selection, initiate the plan enrollment process / electronic transaction to applicable issuers.	W	
EN-18	Eligibility and Enrollment	Plan Selection	OneGate	OneGate	If individuals directly enroll in health plans through the issuer, update an individual's account information based on enrollment information provided by the issuer.	W	out of scope
EN-19	Eligibility and Enrollment	Enrollment	Healthation	Healthation	Prepare an electronic, real-time transmission of information necessary in order for the qualified health plan issuer to provide a welcome package and identification card to the individual and to implement advance premium tax credits and cost-sharing reductions, as applicable.	W	
EN-20	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Record and store current plan enrollment information for all individuals registered on the Exchange.	S	

Individual Enrollment Requirements Traceability Matrix

EN-21	Eligibility and Enrollment	Enrollment	Healthation	Healthation	Process in real-time, the electronic confirmation / acknowledgement of receipt of enrollment transaction from issuer.	W	
EN-22	Eligibility and Enrollment	Enrollment	Healthation	Healthation	Prepare an electronic notice to CMS with a minimum dataset of information regarding an individual's enrollment in a qualified health plan through the Exchange, following the receipt of acknowledgement from the issuer.	W	
EN-23	Eligibility and Enrollment	Enrollment	Healthation	Healthation	Prepare and electronic, real-time electonric transmission to the issuer of an individual's selected qualified health plan regarding changes to the individual's information, including to his or her levels of advance premium tax credits or cost-sharing reductions, or regarding a decision by an individual to	W	
EN-24	Eligibility and Enrollment	Enrollment	Healthation	Healthation	Process in real-time, the electronic confirmation / acknowledgement of receipt of enrollment changes received by an issuer.	W	

Individual Enrollment Requirements Traceability Matrix

EN-25	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Provide capability to receive electronic notifications from issuers regarding disenrollment and initiate disenrollment process	W	
EN-26	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Provide the capability for an individual to request a voluntary disenrollment from a QHP.	W	
EN-27	Eligibility and Enrollment	Enrollment	OneGate	OneGate	If conditions for a voluntary disenrollment (e.g. issuer notifies Exchange of failure to pay QHP premiums beyond the grace period, Issuer or Exchange reports a change in eligibility, etc.), initiate the disenrollment process.	W	
EN-28	Eligibility and Enrollment	Enrollment	OneGate	OneGate	If an individual initiates a voluntary disenrollment through the Exchange and not directly with the Issuer, produce an electronic notification to the Issuer to disenroll an individual.	W	

Individual Enrollment Requirements Traceability Matrix

EN-29	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Update user accounts based on disenrollment notification from issuers or disenrollments initiated by the Exchange.	W	
EN-30	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Prepare a notice to CMS with a minimum dataset of information regarding an individual's disenrollment from a qualified health plan through the Exchange.	W	
EN-31	Eligibility and Enrollment	Enrollment	OneGate	OneGate	When a plan is decertified, initiate the health plan enrollment process for affected individuals (based on special enrollment period rules).	W	
EN-32	Eligibility and Enrollment	Enrollment	OneGate	OneGate	After an individual has been determined eligible to select a QHP, determine the next available period for open enrollment. The open enrollment period should be tracked separately from timeframes for eligibility renewals for Medicaid/CHIP/BHP/Tax Credits.	W	

Individual Enrollment Requirements Traceability Matrix

EN-33	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Prepare and provide communication to individuals about a mid-year plan decertification and notify need for plan selection / enrollment.	W	
EN-34	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Prepare written notification to individuals regarding eligibility for enrollment periods.	W	
EN-35	Eligibility and Enrollment	Enrollment	OneGate	OneGate	Prepare on-screen notification to individuals regarding eligibility for enrollment periods.	W	
EN-36	Eligibility and Enrollment	Periodic Reporting	Business Objects	Oracle BI	Periodically and on an ad hoc basis provide electronic report to issuers about individual QHP enrollment data	M	The CGI team will develop the Vermont specific reports through Oracle BI tools.

Individual Enrollment Requirements Traceability Matrix

EN-37	Eligibility and Enrollment	Periodic Reporting	Healthation	Premium Processor / One Gate	Automatically identify and process issuer discrepancies and payment information	W	Will revisit. Will not be Healthation.
EN-38	Eligibility and Enrollment	Periodic Reporting	Business Objects	Oracle BI	Generate report of periodic issuer reconciliation to CMS	M	The CGI team will develop the Vermont specific reports through Oracle BI tools.
EN-39	Eligibility and Enrollment	Periodic Reporting	OneGate	OneGate	Generate annual report to individual about QHP enrollment	W	
EN-40	Eligibility and Enrollment	Periodic Reporting	Business Objects	Oracle BI	Generate annual report to IRS about QHP enrollment	M	The CGI team will develop the Vermont specific reports through Oracle BI tools.

Individual Enrollment Requirements Traceability Matrix

Plan Management Requirements Traceability Matrix

PM-1	Plan Management	N/A	Oracle Policy Automation, Siebel	OneGate	Provide a business rules engine that can support Exchange, State and federal Plan Management rules	S	
PM-2	Plan Management	N/A	Oracle Policy Automation, Siebel	OneGate	Provide a business rules engine that allows trained authorized business users to configure Exchange rules	S	
PM-3	Plan Management	N/A	CGI Plan Management	OneGate	Provide the ability define a begin and end date for a plan enrollment period	W	
PM-4	Plan Management	N/A	CGI Plan Management	OneGate	Allow for multiple enrollment periods during a calendar year.	W	
PM-5	Plan Management	N/A	CGI Plan Management	OneGate	Provide the ability open a special enrollment period to enable enrolling a plan outside the defined enrollment period.	W	

Plan Management Requirements Traceability Matrix

PM-6	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide the ability, upon request, to generate, publish and send Issuers an electronic Request for Notification of Intent to Apply for QHP certification. Requests will include instructions for application submission.	W	
PM-7	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide the ability for Issuers to submit an electronic Notification of Issuer's Intent to Apply, including all mandatory information	W	RFP processor - year one thru serff, after not clear, do want to have a way to select the plans. No outside market. Must sell thru state.
PM-8	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide Issuers with the ability to initiate an application for Issuer certification and be directed to application requirements	W	
PM-9	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide the ability to capture and store at a minimum the following Issuer information as part of the Notification of Intent to Apply: - Issuer ID - NAIC Number	W	
PM-10	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide the ability to receive, store and track the information included in the Notification of Issuer's Intent to Apply	W	

Plan Management Requirements Traceability Matrix

PM-11	Plan Management	Initiate QHP Issuer App	CGI Plan Management	Manual	Provide interface/query to state database and/or state License system in order to validate Issuer information	C	Out of scope.
PM-12	Plan Management	Initiate QHP Issuer App	CGI Plan Management	Manual	Provide the ability to electronically notify Issuer of validation or non-validation	W	Out of scope.
PM-13	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide the ability to establish and/or verify the existence of an Issuer ID	W	NAIC code generally used currently. Come over via SERFF? Likely. Establish not in scope. Accept is likely later. You are in and have an
PM-14	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Provide Exchange staff the ability to verify Issuer licensure online and in real-time	W	Out of scope.
PM-15	Plan Management	Initiate QHP Issuer App	CGI Plan Management	Manual	Provide the ability to notify the Issuer when an ID has been established	W	Out of scope.

Plan Management Requirements Traceability Matrix

PM-16	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Allow Issuers to initiate product submissions for licensure, for products to be offered both inside and outside the Exchange	W	Form file - is thru serff. Out of scope. (? Once in, which piece of information / product / SOV presents via the exchange / one gate?
PM-17	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Allow the issuer to classify applications to indicate Issuer type: licensed to sell outside the Exchange OR licensed to sell inside and outside the Exchange	W	Out of scope.
PM-18	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Allow the issuer to classify applications to indicate Product type: qualified to sell outside Exchange Or inside and outside the Exchange Market type: Individual market, small group, large group, Medicaid	W	Out of scope.
PM-19	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Allow the issuer to classify applications to indicate Exchange Market type: Individual market, small group, large group, Medicaid	W	Medicaid? How is medicaid getting there? Thru the MMIS process stays in place. Still need to present info on Medicaid. Middleware
PM-20	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Provide the ability to record multiple counties and multiple zip codes by plan to reflect the geographic service area covered by a plan	W	Out of scope.

Plan Management Requirements Traceability Matrix

PM-21	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide multiple levels of categorization of plans to identify different plan 'types' and allow for multiple types of plans (e.g. Line of Business, PPO vs. HMO, Pre-Paid 7A/7B, etc.)	W	show if medicaid plan
PM-22	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide ability to identify those plans that contain pediatric essential dental benefit	W	form review - dfr / reviewed in SERFF. Show at the end in the One Gate - yes.
PM-23	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide ability to identify those plans that contain pediatric essential vision benefit	W	form review - dfr / reviewed in SERFF. Show at the end in the One Gate - yes. Template may need to be modified.
PM-24	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide the capability for issuers to submit QHP certification, recertification, and decertification information in multiple formats including batch upload in a format determined by the Exchange, and	W	Out of scope.

Plan Management Requirements Traceability Matrix

PM-25	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Provide the ability to receive data from issuers on at least the following elements: issuer characteristics, product design and rating rules for approval.	W	SERFF - data transfer of the results - but the initiate is out of scope
PM-26	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Store information about each issuer and product plan offered within the Exchange, as required to support issuer and product plan certification and analysis. Examples of product plan data includes:	W	history - store in data store from SERFF / federal solution uses same templates
PM-27	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	Be able to display a variety of data about a plan to help determine the decision to renew including: - Performance Data - Quality Data - Complaint Data - Coverage data - Benefits and rates	W	RFP process every year? Workflow process? If so, then out of scope. Exchange does not renew - accept the results from external.
PM-28	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	The system must allow the Exchange staff to indicate which plans will be requested to be renewed and which will not.	W	Out of scope.

Plan Management Requirements Traceability Matrix

PM-29	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	The system must, upon request, generate and send electronic renewal request to Issuers about the plans desired to be renewed, requesting an notification of intent to renew.	W	Out of scope.
PM-30	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	The system must be able to receive notifications from Issuers regarding intent to renew or not renew a plan	W	Out of scope.
PM-31	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Proposed solutions may include storage and maintenance of provider networks, or may include functionality to provide a hyperlink to issuer databases. If the option is chosen to store provider networks, the system	W	hyperlink - so out of scope
PM-32	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Provide the ability to evaluate networks against specific criteria as defined by the Exchange	W	Out of scope.
PM-33	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Provide ability to link consumer queries to Issuer databases and state data sets	W	Out of scope.

Plan Management Requirements Traceability Matrix

PM-34	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Capture and store Provider Information including: - Provider type - Accepting new patients y/n - Provider demographic information - Provider services information	W	Out of scope.
PM-35	Plan Management	Initiate QHP Issuer App	CGI Plan Management	N/A	Provide ability to validate an Issuer's certification to sell products within the State including but not limited to: - Issuer Identifier - State Certification Status - Certification date	W	Out of scope.
PM-36	Plan Management	Initiate QHP Issuer App	Oracle SOA Suite Suite	N/A	Provide the ability for Issuers to link information submitted in the Exchange system with information submitted separately to the Insurance Division for other regulatory requirements	W	out of scope. Issuers do not get in. State manages.

Plan Management Requirements Traceability Matrix

PM-37	Plan Management	Initiate QHP Issuer App	CGI Plan Management	SERFF	Provide ability to store Issuer information provided by Insurance Division into the Exchange system. Data can include: - Certification information - Plan approval - Market Analysis results - Audits - Rate Reviews - Quarterly Performance Data - Suspensions or actions (if exist)	W	Need to inherit and display from SERFF.
PM-38	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	SERFF	Provide ability for Exchange staff, and other authorized entities (e.g. Division of Medicaid, Insurance Division, etc. staff) to view Issuer and Plan information, update as needed and add additional data to support plan evaluation.	W	Some difference in consumer / Medicaid so leave in and revisit.
PM-39	Plan Management	Evaluate QHP Issuer Application	Oracle SOA Suite	N/A	Provide the ability via an electronic interface with the appropriate state database resources to validate state insurance licensure, solvency and good	C	out of scope

Plan Management Requirements Traceability Matrix

PM-40	Plan Management	Evaluate QHP Issuer Application	Oracle SOA Suite	SERFF	Provide interface/query capability with the appropriate CMS systems for plan management and financial management functions to return data about an Issuer. Examples of the data include, but are not limited to: - Premium review results - Complaints - Rates of app denial - Claims processing timeliness - Claims denials - Quality reporting	C	Needs to be refined and review after consumer complaint. Quality is from SERFF, the other components, not clear. Backburner issue - 2016. Appeals and grievances - eligibility but not about the doctor refusing to provide service. Commerical is thru DFR currently. Medicaid is not. This is not an interface.
PM-41	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	SERFF	Provide ability to separately approve or disapprove at least the following dimensions of an application: an issuer, a product and rates as separate and distinct elements of certification/recertification/decertification for each market segment (small group, individual).	W	processing of serff data will drive this and review later - federal templates

Plan Management Requirements Traceability Matrix

PM-42	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Provide ability for Issuers to provide relevant Complaint and Compliance Information	W	out of scope - dfr bat phone
PM-43	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	SERFF	Provide ability for authorized users to view product information, request supplemental information, update as needed and add additional data to support product evaluation.	W	pending further discussion
PM-44	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	SERFF	Provide the ability to define a series of criteria fields that will be used to compare and rate plans. Criteria fields can be a variety of types including but not limited to: - True/false or Yes/No - Numerical values for use in calculations - Numerical range fields (example: between x and x values) - Text based fields for narrative criteria - Fields that allow multiple values (text or number)	W	pending further discussion

Plan Management Requirements Traceability Matrix

PM-45	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management		Provide the ability to accommodate time-base criteria to support a defined timeframe for which the criteria is valid	W	check with HI on this requirement, 1/3 - *Hawaii additional clarification - addresses workflow time frames for actions that need to*
PM-46	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management		Store historical criteria which is no longer in active use, or has expired for reference	W	pending further discussion
PM-47	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management		Provide ability for Plan Management workers to compare a proposed exchange plan portfolio to determine if there are gaps missing in coverage, network adequacy, tiers or other criteria.	W	pending further discussion
PM-48	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management		Provide the ability for Plan Management workers to verify Attestations and supporting documentation	W	pending further discussion
PM-49	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management		Allow Plan Management workers to compare a proposed product portfolio against a set of criteria. Possible criteria would include, but not be limited to: - Complaint and Compliance	W	pending further discussion

Plan Management Requirements Traceability Matrix

PM-50	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management		Accommodate variations in criteria by Market (individual, small group, large group).	W	pending further discussion
PM-51	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Accommodate variations in criteria by Issuer type (Exchange / Non-Exchange).	W	out of scope
PM-52	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Provide functionality to track the QHP review workflow process. For example, the system will provide the ability to assign review tasks, note completion, and utilize checklists for review.	W	out of scope
PM-53	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Provide the ability to compile Issuer and product plan application evaluation results	W	out of scope
PM-54	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Provide the ability to electonically send Notice of Application Status to Issuer	W	out of scope

Plan Management Requirements Traceability Matrix

PM-55	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management		Provide the ability to distinguish plans and issuers certified for the Exchange from those that have applied but were denied; those that have expired or decertified.	W	certification is separate from selection for sale. Revisit about displaying or not.
PM-56	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Provide authorized users the ability to enter and store reasons for acceptance or denial of a plan or Issuer into the Exchange	W	out of scope - certified / not selected
PM-57	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Provide the ability to automatically generate formal letter of denial indicating that an Issuer and/or Plan has not been accepted into the Exchange	W	out of scope
PM-58	Plan Management	Evaluate QHP Issuer Application	CGI Plan Management	N/A	Provide the ability to generate letters though all stages of review process (including an electronic form of the letter) of denials; indicating that a issuer and/or productplan has/has not been accepted into the specific market	W	out of scope
PM-59	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	SERFF	Provide the ability to receive and process Rate and Benefit Data for each product plan offered both inside and outside the Exchange	W	templates - serff network

Plan Management Requirements Traceability Matrix

PM-60	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Ability to send notification to Issuers to submit rate and benefit information	W	out of scope
PM-61	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Provide Issuers with the ability for Issuers to provide rate and benefit information in multiple formats including file upload in a format determined by the Exchange, and direct data entry.	W	out of scope
PM-62	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Allow benefit data to be collected in discrete elements, as defined by federal guidance and state requirements. For example, each category and subcategory of Essential Health Benefits must appear, along	W	out of scope
PM-63	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Allow Issuers to classify product plans as QHP-applicable and non-QHP-considered; and also classify within a market type (e.g. individual, small group, large group, etc.)	W	QHP / public - out of scope - the other categories do not exist here
PM-64	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Provide the ability to receive rate tables *and/or* rating rules in multiple formats including electronic file in a format determined by the Exchange, and direct data entry.	W	out of scope

Plan Management Requirements Traceability Matrix

PM-65	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Peform data validation on rate/benefit data to ensure accuracy and completeness of supplied data.	W	out of scope
PM-66	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Provide electronic notification to Issuers regarding data issues related to rate and benefit information submission(s)	W	out of scope
PM-67	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Provide electronic notification to Issuer to provide Final Attestation for Rate/Benefit Data and Information	W	out of scope
PM-68	Plan Management	Rate and Benefit Information Receipt	CGI Plan Management	N/A	Allow Insurance Issuers the ability to provide premium information in real-time or as part of the catalog in a batch upload.	W	out of scope
PM-69	Plan Management	Revise QHP Issuer Application	CGI Plan Management	N/A	Provide Issuer the ability to withdraw an application for consideration for individual, small or large group market, and/or consideration in individual exchange and/or SHOP exchange	W	out of scope

Plan Management Requirements Traceability Matrix

PM-70	Plan Management	Determine Issuer Plan Non-Certification	CGI Plan Management	SERFF	Provide the ability to record the plan non-renewal event and status information, including date, reason/rationale	W	? Six month withdrawl process - need to mark for a future withdrawl
PM-71	Plan Management	Determine Issuer Plan Non-Certification	CGI Plan Management	N/A	Produce electronic and/or paper notices to Issuers when a plan is decertified from Exchange	W	out of scope
PM-72	Plan Management	Determine Issuer Plan Non-Certification	CGI Plan Management	N/A	Provide the ability to record the plan or issuer decertification event and status information, including date, reason/rationale	W	out of scope
PM-73	Plan Management	Determine Issuer Plan Non-Certification	CGI Plan Management	N/A	Produce electronic notification to Insurance Division when a Issuer/plan is not renewed or is decertified from the Exchange	W	out of scope
PM-74	Plan Management	Determine Issuer Plan Non-Certification	CGI Plan Management	SERFF	Produce electronic notification to CMS when an Issuer/plan is not renewed or is decertified from the Exchange	W	need it - dfr decertifies - workflow for notice needs to be worked out. Renewal different.

Plan Management Requirements Traceability Matrix

PM-75	Plan Management	Determine Issuer Plan Non-Certification	CGI Plan Management	SERFF	Provide the ability to define an option period for recertification and renewal.	W	out of scope
PM-76	Plan Management	Determine Issuer Plan Non-Certification	CGI Plan Management	SERFF	Send notification to the Insurance Division or other relevant state agencies of those Isssuers and/or Plans which have been denied acceptance to participate in the Exchange.	W	out of scope
PM-77	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	N/A	Provide the ability to open a special certification period to enable certifying an Issuer or Plan outside the defined certification period	W	out of scope
PM-78	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	N/A	Provide the ability to record agreement information in the system including: - Agreement ID - Agreement begin date - Agreement end date - Plan Operations begin date - Plan Operations end date	W	Agreements are contracts, not a different document. So this would be paper and documented with the contract. Out of scope.

Plan Management Requirements Traceability Matrix

PM-79	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	N/A	Provide the ability to generate a notification of certification into the Exchange	W	out of scope - manual
PM-80	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	N/A	Allow storage of agreement signature or acceptance date to indicate the Issuer agreement acceptance.	W	out of scope - manual
PM-81	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	N/A	Provide ability to store an electronic copy of the agreement and associate it with a plan record so it can be retrieved and viewed when querying information about a plan.	W	out of scope - manual
PM-82	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	SERFF	Determine the quality rating in accordance with CMS plan quality rating methodology.	W	Need to address a quality rating - display - yes. Create? Not clear.
PM-83	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	SERFF	Determine the medal rating of a plan (platinum, gold, silver, bronze)	W	no - not determine, but display (catestrophic tier medal)

Plan Management Requirements Traceability Matrix

PM-84	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	SERFF	Provide query of plans by issuer with calculated rating for other attributes to be determined by the Exchange.	W	out of scope
PM-85	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management		Provide the ability for plan information to be 'published' to the public exchange view when approval for plan is finalized	W	when selected - three step - approved for sale is viewable

Plan Management Requirements Traceability Matrix

PM-86	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management		Provide the ability to display plan information on the public exchange view, including, but not limited to data such as: - Plan title and description - Plan quality rating - Plan providers - Out of pocket limits - Annual deductable - Doctor Choice - Prescription Choice - Monthly Premium - Applicants Denied - Plan Details - Link to Issuer/Plan website - Medical loss ratio - Transparency in coverage - Summary in benefits and coverage - Levels of coverage - Availability of in-network and out-of-network providers	W	confirmed need
PM-87	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management		Provide the ability for plan information to be easily removed from the public exchange view if approval status of the plan changes	W	confirmed need

Plan Management Requirements Traceability Matrix

PM-88	Plan Management	Establish QHP Certification and Agreement	Oracle SOA Suite	N/A	Provide electronic data to the Insurance Division to indicate notice of issuers/plans approved for the Exchange. Data can include: - Issuer ID - Exchange certification date	W	out of scope
PM-89	Plan Management	Establish QHP Certification and Agreement	CGI Plan Management	N/A	Provide the ability to store an electronic copy of the agreement and associate it with a plan record so it can be retrieved and viewed when querying information about a plan	W	out of scope
PM-90	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	Support receipt of recertification data in the same manner used for initial certification.	W	out of scope
PM-91	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	Support storage, view and processing of recertification data and analysis in the same manner used for initial certification.	W	out of scope

Plan Management Requirements Traceability Matrix

PM-92	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	Distinguish if data and tracking activities are for initial certification or recertification	W	out of scope
PM-93	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	SERFF	Store and provide the capability to display on demand transactional history related to the QHP certification plrocess, inlcuing but not limited to certification/decertification event and rationale for decertification events.	W	yes - for the history of offered plans
PM-94	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	SERFF	Store a record of all QHP negotiation steps, activities, and outcomes.	W	out of scope - as separate step - in SERFF
PM-95	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	SERFF	Generate re-amendment notification and information storage consistent with the initial certification amendment process.	W	out of scope - as separate step - in SERFF

Plan Management Requirements Traceability Matrix

PM-96	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	SERFF	Process agreement acceptance from Issuers consistent with the initial certification acceptance process	W	out of scope - as separate step - in SERFF
PM-97	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	SERFF	Update Issuer and agreement information in the system consistent with the initial certification amendment process.	W	out of scope - as separate step - in SERFF
PM-98	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	Recertify the plan and notify issuers consistent with the initial certification process.	W	out of scope
PM-99	Plan Management	Establish Issuer and Plan Renewal and Recertification	Oracle SOA Suite	SERFF	Update CMS with certified plan information consistent with the initial certification process	W	To be dealt with in reports to CMS (in SERFF)
PM-100	Plan Management	Establish Issuer and Plan Renewal and Recertification	CGI Plan Management	N/A	The system must distinguish to CMS initial certified data from recertified plan data.	W	out of scope

Plan Management Requirements Traceability Matrix

PM-101	Plan Management	Collect and Aggregate Plan Data	Oracle SOA Suite	SERFF	Provide functionality to periodically submit required data to the appropriate CMS system for plan management and fiscal management functions including but not limited to reporting on the following data:	W	To be dealt with in reports to CMS (in SERFF)
PM-102	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management	N/A	Provide the ability to define performance monitoring periods (i.e. quarterly, monthly etc.)	W	DFR does the license - they set up their own mechanisms - separate workflow
PM-103	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Accept Issuer and plan performance data electronically from Issuers and the Insurance Division in support of periodic monitoring activities such as: - HEDIS ratings - Consumer perception ratings (CAPS) - Complaints - Patient information programs - Claims payment data - Disenrollment data - Denied claims - Issuer ID - Compliant data/summaries	W	Accept from insurance - may want it. Monitor - not done thru exchange. There is a requirement about the denials. We need to revisit.

Plan Management Requirements Traceability Matrix

PM-104	Plan Management	Monitor Issuer/Plan Compliance	Business Objects	Reporting	Provide analytical queries and reports to analyze plan compliance and monitoing data	M	The CGI team will develop the specific reports through Business Objects. We may need to revisit the performance elements. See above.
PM-105	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Accept Issuer and Plan data electronically from CMS in support of periodic monitoring activities such as: -Issuer ID -Plan ID -Complaint data/summaries -Other data to be determined by CMS	C	Not clear what CMS will be providing and then do not know what accepting and how to use - interfaces will address and need to be revisited.
PM-106	Plan Management	Monitor Issuer/Plan Compliance	Business Objects	Reporting	Provide the ability to analyze and report on performance data provided by Issuers	C	The CGI team will develop the specific reports through Business Objects. We may need to revisit the performance elements. See above.

Plan Management Requirements Traceability Matrix

PM-107	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management	Reporting	Track the receipt of performance and compliance data from Issuers and including date of receipt	W	repeat - see above for the same requirement
PM-108	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management	N/A	Allow authorized users to track receipt of information received by Issuers in non-data formats, i.e. PDFs	W	out of scope

Plan Management Requirements Traceability Matrix

PM-109	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Allow recording results of compliance analysis, and the status of an issuer/plan meeting a variety compliance requirements such as: - Benefits design standards - validation/tracking data - Essential benefits - Cost sharing limits - Coverage levels - Insurance Division certification status - User fee compliance - Risk adjustment participation compliance - Plan offering compliance - Non discrimination compliance - Transparency requirements	W	Revisit later for additional details and not clear who is doing the compliance. Start with CMS data elements. What and who. To the extent that we can - when this conversation occurs again, consider the single payer future needs as well as current data. Data conversation with carriers and other stakeholders.
PM-110	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Indicate the status of an Issuer/Plan compliance determination	W	see pm-109

Plan Management Requirements Traceability Matrix

PM-111	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Allow for preliminary and final compliance determinations	W	see pm-109
PM-112	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Retain historical compliance tracking information	W	see pm-109
PM-113	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Provide a compliance dashboard to indicate compliance analysis progress on Issuers/plans and the results of the compliance analysis through the compliance process	W	out of scope
PM-114	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management	N/A	Provide a Performance indicator dashboard to aggregate performance data and display summary performance information by Issuer/Plan	W	need to revisit
PM-115	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management	Not for October 2013	Calculate a quality rating for each plan according to a methodology determined by the Exchange.	W	display yes, calculate - unclear - not a first year thing

Plan Management Requirements Traceability Matrix

PM-116	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management		Retain historical plan quality ratings	W	yes - for the history of offered plans
PM-117	Plan Management	Monitor Issuer/Plan Compliance	OneGate		Display the most current quality rating for each plan on the consumer website.	W	yes - will display
PM-118	Plan Management	Monitor Issuer/Plan Compliance	CGI Plan Management	N/A	Produce electronic or paper notices for Issuers indicating the results of the compliance and quality reviews, i.e. the compliance and quality rating determination	W	not in scope - unclear - revisit - if exchange does compliance - this need
PM-119	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	The system must accept electronic Issuer complaint data in a secure manner, from the Insurance Division on a monthly basis.	W	customer assistance handles the customer compliant. Manual.
PM-120	Plan Management	Maintain Operational Data	CGI Plan Management		Provide the ability to receive, store and track electronic Issuer and Plan complaint data from the appropriate CMS system for plan management and fiscal management functions on a periodic basis. Complaint data can	W	Pending CMS clarity

Plan Management Requirements Traceability Matrix

PM-121	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide web-based interface for Exchange consumers, providers, brokers, navigators, etc. to enter complaints about Exchange Issuers and/or Plans will capture complaint data including: - Exchange user id (for consumers, navigators, etc.) - Provider id (for providers) - Issuer - Plan - Complaint description/detail - Complaint type - Complaint source	W	Who is recording the complaint? VT statute has expectations. There needs to be a handoff - reflect how the business workflow should function and figure out the communication. Revisit with the consumer assistance requirements. Compliants / appeals from the different views.
PM-122	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide automatic electronic notification of receipt for complains submitted through the web interface.	W	See pm-121
PM-123	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Allow Exchange users such as consumers, navigators, etc. to log into their Exchange account to post/submit a complaint	W	see pm-121

Plan Management Requirements Traceability Matrix

PM-124	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the ability to accept electronic Issuer/Plan complaint data in secure manner, from Exchange Issuers on a periodic basis. Complaint data can include: - Issuer	W	see pm-121
PM-125	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Track and manage complaints for the Exchange	W	see pm-121
PM-126	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Use a common, standard format for complaint data from all sources to facilitate merging complaint data for analysis.	W	see pm-121
PM-127	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Allow complaint managers to classify complaints by attributes to support triaging complaints for action or referral	W	see pm-121
PM-128	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Retain the source of the complaint (i.e. provider, issuer, Insurance Division, etc.) and the date received	W	see pm-121

Plan Management Requirements Traceability Matrix

PM-129	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Users must have a way to aggregate or combine multiple versions of the same complaint or relate multiple complaints to a single complaint case	W	see pm-121
PM-130	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Track and manage activities related to researching and addressing complaints from complaint receipt to completion/resolution of a complaint including who took action, what the action was, relevant dates,	W	see pm-121
PM-131	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability to auto-assign a complaint to a complaint worker or account manager based on information provided in the complaint	W	see pm-121
PM-132	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Notify a complaint worker that a complaint has been assigned/routed to that person	W	see pm-121
PM-133	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Allow reassignment of a complaint to a new complaint worker	W	see pm-121

Plan Management Requirements Traceability Matrix

PM-134	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide queries/reports to track and manage complaint workload, disposition, assignments and status	W	see pm-121
PM-135	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide sorts/reports/queries to support summarizing and analyzing complaints and complaint trends by a variety of complaint data attributes.	W	see pm-121
PM-136	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Publish approved complaint data summaries on the Exchange web portal for customer review , and to support transparency.	W	see pm-121
PM-137	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide electronic Exchange Issuer complaint data to the Insurance Division on a periodic basis. Complaint data can include: - Issuer - Number of complaints	W	see pm-121
PM-138	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability to send an electronic complaint referral to: - An Issuer - OIC - Eligibility case/complaint workers - Exchange customer service	W	see pm-121

Plan Management Requirements Traceability Matrix

PM-139	Plan Management	Maintain Operational Data	CGI Plan Management		Allow Issuers to submit new/changed marketing and Enrollee communication materials	W	nice to have
PM-140	Plan Management	Maintain Operational Data	CGI Plan Management		Receive electronic files of marketing materials from Issuers	W	nice to have
PM-141	Plan Management	Maintain Operational Data	CGI Plan Management		Allow users must be able to classify marketing materials from Issuers	W	nice to have
PM-142	Plan Management	Maintain Operational Data	CGI Plan Management		Store and track electronic files of marketing materials from Issuers	W	nice to have
PM-143	Plan Management	Maintain Operational Data	CGI Plan Management		Allow Plan Management staff to view electronic files of marketing materials	W	nice to have

Plan Management Requirements Traceability Matrix

PM-144	Plan Management	Maintain Operational Data	CGI Plan Management		Track review and approval activities related to review of marketing materials	W	nice to have
PM-145	Plan Management	Maintain Operational Data	CGI Plan Management		Allow Marketing materials to be linked to appropriate plan/issuer records in the system.	W	nice to have
PM-146	Plan Management	Maintain Operational Data	CGI Plan Management		Provide capability to categorize marketing materials according to a schema defined by the Exchange	W	nice to have
PM-147	Plan Management	Maintain Operational Data	CGI Plan Management		Provide the ability to store links to websites that are references to marketing materials. The links must be able to be associated to appropriate Issuers/Plans.	W	nice to have
PM-148	Plan Management	Maintain Operational Data	CGI Plan Management		Track marketing material revision requests and the revision process, including tracking data about revision requests such as - Issuer Identifier - Plan Identifier	W	nice to have

Plan Management Requirements Traceability Matrix

PM-149	Plan Management	Maintain Operational Data	CGI Plan Management		Provide version control document management capabilities for submitted marketing materials in order to manage document submissions and revisions	W	nice to have
PM-150	Plan Management	Maintain Operational Data	CGI Plan Management		Allow marketing material reviewers to create and send notifications to Issuers about requested revisions	W	nice to have
PM-151	Plan Management	Maintain Operational Data	CGI Plan Management		Record approval information about marketing materials, including: -Approver -Approve Date -Status	W	nice to have
PM-152	Plan Management	Maintain Operational Data	CGI Plan Management		Upon approval of marketing materials, generate notification to Issuer regarding approval	W	nice to have
PM-153	Plan Management	Maintain Operational Data	CGI Plan Management		Upon approval of marketing materials, provide update to Isssuer's QHP Account Information	W	nice to have

Plan Management Requirements Traceability Matrix

PM-154	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide the ability for Issuers to submit Provider Network Information	W	out of scope
PM-155	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide ability for Exchange staff to view Provider information, update as needed and add additional data not provided electronically.	W	out of scope
PM-156	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Accept electronic Provider network information by Issuer from the Insurance Division on a monthly basis. Provider data can include: - Issuer data - Provider data	W	out of scope
PM-157	Plan Management	Maintain Operational Data	Business Objects	N/A	Provide analytic tools/reports/queries to support determining provider coverage adequacy of a plan by a variety of complaint data attributes including adequate coverage by geography and specialty	M	out of scope

Plan Management Requirements Traceability Matrix

PM-158	Plan Management	Maintain Operational Data	Business Objects	Reporting	The system must provide analytic tools/reports/queries to support determining Issuer/plan compliance with Exchange rules/policy	M	refer to BI tool
PM-159	Plan Management	Maintain Operational Data	Business Objects	Reporting	The system must provide analytic tools/reports/queries to support determining provider coverage adequacy of the Exchange plan portfolio by a variety of complaint data attributes.	M	Redundant with pm-158
PM-160	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Upon authorized approval, the updated Provider Network for a plan or Issuer must be able to be published to the Exchange website for view by consumers.	W	out of scope
PM-161	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide the ability for historical Provider data must be saved to provide accurate historical representation of the Provider network at a given point in time	W	out of scope

Plan Management Requirements Traceability Matrix

PM-162	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide notices to be sent to plan consumers, Navigators and brokers if a Provider Network change requires consumer notification, according to rules defined by the Exchange.	W	out of scope
PM-163	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide ability for Insurance Issuer staff to view Provider information, update as needed and add additional data. It is anticipated that Issuers will have access to less Plan data fields that Exchange staff. Data may include:	W	out of scope
PM-164	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Notify authorized Exchange users when an Issuer has updated any Issuer, plan and provider data	W	out of scope
PM-165	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide the ability for authorized Exchange user to view changes made by a Issuer to Issuer, Plan and Provider data	W	out of scope
PM-166	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide ability for an authorized Exchange user to authorize changes made by a Issuer to be posted to the exchange.	W	out of scope

Plan Management Requirements Traceability Matrix

PM-167	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Store and track historical Issuer administrative data	W	out of scope - not clear
PM-168	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide ability for Issuers to electronically submit transparency and quality data such as: - Issuer Identifier - Transparency/quality Information: - Payment policies and practices	W	Rule 903 - Excel spreadsheets. Revisit later? Out of scope for now.
PM-169	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	Provide the ability to receive electronic documents of transparency or quality information from Issuers	W	Rule 903 - Excel spreadsheets. Revisit later? Out of scope for now.
PM-170	Plan Management	Maintain Operational Data	Business Objects	N/A	Provide tools/sorts/reports/queries to support summarizing and analyzing transparency and quality data	S	Rule 903 - Excel spreadsheets. Revisit later? Out of scope for now.

Plan Management Requirements Traceability Matrix

PM-171	Plan Management	Maintain Operational Data	CGI Plan Management	N/A	The system must be able to track the review steps and progress of transparency and quality data analysis including: - When information was received - Analytical steps - Process status	W	Rule 903 - Excel spreadsheets. Revisit later? Out of scope for now.
PM-172	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management	N/A	Issuers must be able to electronically communicate a plan enrollment change to the Exchange system. Data required will include: - Enrollment availability status - Change justification - Effective dates - Status indicating if new dependent enrollee's are still allowed	W	out of scope

Plan Management Requirements Traceability Matrix

PM-173	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management	SERFF	The Insurance Division must be able to electronically communicate a plan enrollment change to the Exchange system. Data required will include: - Enrollment availability status - Change justification - Effective dates - Status indicating if new dependent enrollee's are still allowed	W	stays in scope
PM-174	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management	N/A	Provide the ability to record the request for change in product availability including: - Issuer Identifier - Plan Identifier - Plan Changes Effective Date - Changed Plan Information: - Enrollment close status - Enrollment open status - Justification information - Requestor information - Status of change request	W	out of scope - request goes to dfr and dfr sends to exchange. MMIS to exchange.
PM-175	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management	N/A	Provide automatic notification to authorized Exchange users indicating that an enrollment request has been received.	W	out of scope

Plan Management Requirements Traceability Matrix

PM-176	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management		Provide the Exchange Plan Account Manager with the ability to review enrollment change request data and electronically approve or disapprove the enrollment notification or request.	W	in scope
PM-177	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management		Upon approval of the enrollment change request, generate an electronic notification to the Insurance Division indicating the plan enrollment status	W	wording is odd - if a plan change occurs - dft would be informing the exchange - notify members / not insurers - not happening
PM-178	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management	N/A	Upon approval of the enrollment change request, generate an electronic notification to Exchange Issuers indicating the plan enrollment status	W	see pm-177 = same - out of scope
PM-179	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management		Upon approval of the enrollment change request, generate an electronic notification to registered Navigators/Brokers indicating the plan enrollment status	W	need to notify brokers and public - issuer is dfr..

Plan Management Requirements Traceability Matrix

PM-180	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management	SERFF	Upon approval of the enrollment change request, send an update transaction to the appropriate CMS system for plan management and fiscal management functions indicating the plan enrollment status	W	in scope
PM-181	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management	N/A	Upon approval or disapproval of the enrollment change request, generate notification to the requesting Issuer.	W	out of scope
PM-182	Plan Management	Process Change in Plan Enrollment Availability	CGI Plan Management		Allow authorized Navigators/Brokers to manage subscriptions to appropriate Exchange notification functions and features	W	review in the broker and navigator session
PM-183	Plan Management	Issuer Account Mgt	Identity Management	N/A	The system must allow issuers to create and manage user accounts.	W	out of scope
PM-184	Plan Management	Issuer Account Mgt	CGI Plan Management	N/A	Certified issuers shall have the ability to list their QHPs in the Exchange catalog and present information on them.	W	out of scope

Plan Management Requirements Traceability Matrix

PM-185	Plan Management	Issuer Account Mgt	CGI Plan Management	N/A	Certified issuers shall have the ability to access the Exchange catalog and make updates to the products offered following formal approval of those updates by the State.	W	out of scope
PM-186	Plan Management	Issuer Account Mgt	CGI Plan Management	OneGate	Provide the ability for issuer and product information to be "published" to the public exchange view when approval is finalized.	W	in scope - approval is selected
PM-187	Plan Management	Issuer Account Mgt	CGI Plan Management	OneGate	Provide the ability for issuer and product information to be easily removed from the public exchange view if approval status changes	W	in scope
PM-188	Plan Management	Issuer Account Mgt	CGI Plan Management	SERFF	The system shall periodically submit data to the appropriate CMS system for plan management and fiscal management functions, as required by federal regulation.	W	in scope

Plan Management Requirements Traceability Matrix

PM-189	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Provide ability for Issuers to electronically submit rate and benefit data, and a justification for rate increase. Rate Data may include: - Rate Changes Effective Date - Benefit Data - Discretionary Benefits - Services/Service Categories - Related co-payments/deductibles - Justification for Rate Increase - Changes in Cost - Utilization Changes	W	out of scope - serff
PM-190	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Allow quarterly new enrollee 'trend up' rates to be submitted and stored, including the trend up dates in which the rates would become active.	W	out of scope - serff
PM-191	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Provide the ability to turn a trend up rate on or off, i.e. allow an Issuer to submit a trend up rate but choose not to use it later.	W	out of scope - serff

Plan Management Requirements Traceability Matrix

PM-192	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Screen submitted rate and benefit data and provide formatting error information back to the Issuer if data format is not correct	W	out of scope - serff
PM-193	Plan Management	Review Rate Increase Justifications	Business Objects	SERFF	Provide submitted rate and benefit data to the Insurance Division system and CMS electronically	M	out of scope - serff -
PM-194	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Provide the ability for authorized users to view and utilize proposed rate and benefit data during the analysis of rate justifications.	W	out of scope - serff -
PM-195	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Provide the ability for users to track the steps/progress of rate justification analysis, including steps completed / not completed and dates	W	out of scope - serff -
PM-196	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Allow users to track communications with Issuers and Insurance Division to support the analysis/negotiations process	W	out of scope - serff -

Plan Management Requirements Traceability Matrix

PM-197	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Provide comparisons between current and proposed rates and plan benefits	W	out of scope - serff -
PM-198	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Provide the ability to receive/store/track multiple rate change justifications if multiple are submitted during the negotiation process or after a rate change denial.	W	out of scope - serff -
PM-199	Plan Management	Review Rate Increase Justifications	CGI Plan Management	N/A	If a rate increase is denied, generate a denial notice to the issuer both electronically, and as a formal notice that can be mailed.	W	out of scope
PM-200	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Upon approval of rate increase, generate an approval notice to the issuer both electronically, and as a formal notice that can be mailed.	W	out of scope - serff -
PM-201	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Upon rate increase approval, update certification agreement data and relevant rate and benefit data, effective dates.	W	out of scope - serff

Plan Management Requirements Traceability Matrix

PM-202	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Upon rate approval, send updated plan/rate/benefit data to the appropriate CMS system for plan management and fiscal management functions for determination of silver plans.	W	out of scope - serff
PM-203	Plan Management	Review Rate Increase Justifications	CGI Plan Management	SERFF	Provide the ability to receive and process second lowest cost silver plan ratings from the appropriate CMS system for plan management and fiscal management functions. - Issuer Identifier	W	out of scope - serff
PM-204	Plan Management	Review Rate Increase Justifications	CGI Plan Management	OneGate	Allow the authorized user to publish finalized rates and benefits data to the public facing Exchange.	W	in scope
PM-205	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Track communications with Issuers and the Insurance Division to support the rate review analysis/negotiation process	W	out of scope - serff
PM-206	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	N/A	Track if a rate increase denial is being appealed by an Issuer (upon notification by the Issuer).	W	out of scope

Plan Management Requirements Traceability Matrix

PM-207	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Provide ability for Issuers to re-submit rate and/or benefit information based on Request	W	out of scope - serff
PM-208	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Perform data validation checks on revised rate and/or benefit data and notify Issuer if additional corrections are required	W	out of scope - serff
PM-209	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Provide a notification to Issuer to submit final Attestation	W	out of scope - serff
PM-210	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Provide Issuers with ability to submit final Attestation	W	out of scope - serff
PM-211	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Capture, store and track Issuer's final Attestation	W	out of scope - serff

Plan Management Requirements Traceability Matrix

PM-212	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Determine if Issuer provided rate and/or benefit data and information revisions within the designated time-frame	W	out of scope - serff
PM-213	Plan Management	Revise Rate and Benefit Data	CGI Plan Management	SERFF	Provide electronic and hard-copy notification to Issuer of QHP rate/benefit data and information revision acceptance	W	out of scope - serff

SOV HBE Consolidated Functional Requirements Traceability Matrix (RTM)								
Col Descriptors								
Business Area	Business Process	Req Id	Status	Requirement Description	Cross Refer to Plan Management Tab	Conditions (S, W, M, F, C)		Comments
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement		Functional	The system shall allow QHP admin to select which benefit services are displayed in the web portal from the superset associated to the QHP.	PM-85			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement		Functional	The system shall provide the ability to identify a plan as a High Deductible Health Plan (HDHP)	PM-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement		Functional	Benefits/Services may require effective dates – to be confirmed	PM-59 / PM - 43			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement		Functional	Issuer Status values should include: In Progress Certified Decertified	PM-93			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement		Functional	Plan Benefit Services need ability to store both $ Limit and Max # of Visits. QHP only have Max # Visits, Dental at a plan level has $ Limit and at a benefit level requires both max visits and frequency of visits; public plan benefits will need both $ Limit and Max # of Visits	PM-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement		Functional	Public Plan rate view needs ability to capture separate entries for FPL level, household size, Rate $, and rate effective dates. It's expected that 4-5 FPL levels would exist	Pm-59			

Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	Public Plan Status values should include: In Progress Approved Available Discontinued	PM-93			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	Public plans require an attribute to differentiate 'DeliveryModel'. Options are: Fee for Service and Managed Care	PM-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	QHP Plan Status values should include: In Progress Certified Selected Withdrawn	PM-55			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system should allow for a URL to be stored against the Plan or Plan Benefit for Preferred Drug List Formulary list	PM-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	Plans should allow for at least 5 tiers with different premium levels: Individual, Individual +1, Parent/Child, Child Only, Family	PM-63			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	Siebel to ACCESS interface will be required for Public Plan enrollment data if ACCESS continue to be used for eligibility and determination outputs.	New	C	NA	It is not clear to CGI how this is a plan management functional issue. Currently, this requirement is not a component of the CGI standard solution. This requirement would require a change order.
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	Summary of Benefits shall be reference at the Plan level and provide a URL link to a Issuer maintained website	PM-86			

Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The Exchange shall allow for plans to be characterized as Standard Plans vs Choice Plan	pm-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The Exchange shall allow the ability to setup plans which can be browsed but not available for enrollment (soft launch) based on coverage effective date.	pm-85			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The Exchange web portal should only display plans which have a status of 'Selected'. Plans loaded as 'Certified' but which have not been selected should not be displayed on the web portal.	pm-85			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system shall allow Plan to be setup so they are only visible on the web portal after a specified date	pm-85			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system shall not publish plans which have not been certified AND had rates approved.	pm-87			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system shall provide ability to create, update, and/or analyze issuer and plan information. This applies to initial creation and subsequent updates to information.	pm-38			

Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system shall provide the means for plan administrators to load plans and required content into the Exchange. These means shall include direct data entry via an administrative tool, a real-time or batch interface or a common formatted file.	pm-16			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system shall support the following date elements on a Plan: Publish Start date; enrollment Start/End date; Coverage Start/End date	pm-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system should allow for plans be classified as Certified, Decertified, Selected	pm-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The system will use the NAIC code as a unique identifier for the issuer.	pm-13			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	The web portal for QHPs shall include a URL link to a provider registry website that will be maintained by the Issuer	pm-86			
Plan Management	BP-PM-01: Establish Issuer and Plan Initial Certification and Agreement	Functional	Ability for the system to support Plans with different cost sharing reduction values than the standard silver plan CSRs. Native American may be eligible for CSRs across any metal level and this may require separate plans to be submitted by the Issuers.	pm-21 & pm-83			
Plan Management	BP-PM-02: Monitor Issuer and Plan Certification Compliance	Functional	The system shall provide the functionality to assign an initial quality rating to a Qualified Health plan (QHP).	pm-82			

Plan Management	BP-PM-02: Monitor Issuer and Plan Certification Compliance	Functional	The system shall provide the functionality to update QHP plan quality ratings and track historical ratings and time periods for these ratings (begin and end dates).	pm-93 & pm-116			
Plan Management	BP-PM-03: Establish Issuer and Plan Renewal and Recertification	Functional	The system shall provide the ability to distinguish plans and issuers certified for the Exchange from those that have applied but were denied, those that have expired or decertified.	pm-93			
Plan Management	BP-PM-03: Establish Issuer and Plan Renewal and Recertification	Functional	The system shall provide the ability to enter and store reasons for acceptance or denial of a plan or issuer into the Exchange as a comment	pm-93			
Plan Management	BP-PM-03: Establish Issuer and Plan Renewal and Recertification	Functional	The system shall provide the ability to remove and/or deactivate a decertified plan from the Exchange.	pm-93			
Plan Management	BP-PM-03: Establish Issuer and Plan Renewal and Recertification	Functional	The system shall provide the functionality to decertify an issuer or QHP, should they fail to be compliant with Exchange criteria.	pm-110			
Plan Management	BP-PM-04: Maintain Operational Data	Functional	Public Plan Admin role should not be able to modify QHP plans and Issuer data	pm-176			
Plan Management	BP-PM-04: Maintain Operational Data	Functional	DVHA QHP Admin role should not be able to modify Public plans	pm-176			
Plan Management	BP-PM-04: Maintain Operational Data	Functional	Ability for DVHA Plan administrators to submit and receive changes to Plan data such as: Transparency and Quality, General Issuer Information, and Provider Networks URLs.	pm-176			

Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall notify CMS and CID of change in QHP enrollment availability (open/closed).	pm-180			
Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall provide the ability to hide and unhide plans from consumer view/access according to QHP enrollment availability.	pm-173			
Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall record the plan non-renewal event and status information, including date and reason/rationale.	pm-70			
Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall track all changes to plan availability and pertinent statistics and information associated with the plan.	pm-173			
Plan Management	BP-PM-06: Review Rate Increase Justifications	Functional	Automated update of plan data from SERFF load should be blocked if QHP Status is 'Selected'.	pm-201			
Plan Management	BP-PM-06: Review Rate Increase Justifications	Functional	Rating Tiers shall have start and end dates. Overlapping rating tiers can be entered in the exchange. For example (1/1/2014-12/31/2014) AND (6/1/2014-5/31/15)	pm-59			
Plan Management	BP-PM-06: Review Rate Increase Justifications	Functional	The system shall provide the functionality to revise rates and benefits data submission.	pm-201			

Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall notify CMS and CID of change in QHP enrollment availability (open/closed).	pm-180			
Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall provide the ability to hide and unhide plans from consumer view/access according to QHP enrollment availability.	pm-173			
Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall record the plan non-renewal event and status information, including date and reason/rationale.	pm-70			
Plan Management	BP-PM-05: Process Change in Plan enrollment Availability	Functional	The system shall track all changes to plan availability and pertinent statistics and information associated with the plan.	pm-173			
Plan Management	BP-PM-06: Review Rate Increase Justifications	Functional	Automated update of plan data from SERFF load should be blocked if QHP Status is 'Selected'.	pm-201			
Plan Management	BP-PM-06: Review Rate Increase Justifications	Functional	Rating Tiers shall have start and end dates. Overlapping rating tiers can be entered in the exchange. For example (1/1/2014-12/31/2014) AND (6/1/2014-5/31/15)	pm-59			
Plan Management	BP-PM-06: Review Rate Increase Justifications	Functional	The system shall provide the functionality to revise rates and benefits data submission.	pm-201			

Small Business Requirements Traceability Matrix

SH-3	Small Business	Prepare Employer Application	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide capability for employers to request further assistance through Chat Support (online assistance from a customer service representative) during the preliminary questionnaire process.	S	
SH-4	Small Business	Prepare Employer Application	OneGate	OneGate	Provide multiple methods for an employer to build an employee roster through the application process (e.g. manual entry, file upload, etc.)	S	

Small Business Requirements Traceability Matrix

SH-5	Small Business	Plan Selection/ Employer Application	OneGate	OneGate	Generate a request to initiate the employer selection of qualified health plan during the application process.	S	
SH-6	Small Business	Plan Selection	OneGate	OneGate	Provide the capability to calculate an estimate as to whether a premium might exceed the affordability scale for a given employee income, so that the employer may know the likelihood of receiving a tax penalty for offering unaffordable insurance.	S	

Small Business Requirements Traceability Matrix

SH-7	Small Business	Plan Selection	OneGate	OneGate	Based on carrier and plan information gathered, display plan cost and availability based on initial questionnaire completed by the employer.	S	
SH-8	Small Business	Plan Selection	OneGate	OneGate	As a default, only display health plans that have been certified by the Exchange, are open to additional enrollment, and are available in the employer's geographic area.	W	

Small Business Requirements Traceability Matrix

SH-9	Small Business	Plan Selection	OneGate	OneGate	Display actual plan cost based on applicable rating factors (consumers covered, age, geography, etc.) provided by the employer during the application process.	W	Smoking question needs to be removed
SH-10	Small Business	Plan Selection	OneGate	OneGate	Provide capability to display a detailed comparison of available health plans based on employer preferences, including product categories.	S	

Small Business Requirements Traceability Matrix

SH-11	Small Business	Plan Selection	OneGate	OneGate	Provide capability to display a detailed quality and cost comparison of all available health plans based on information (e.g. gender, age, smoking) about employees and employee dependents listed in the employee roster.	W	
SH-12	Small Business	Plan Selection	OneGate	OneGate	Provide capability for employers to adjust employer preferences and update display / comparison of available qualified health plans. This capability includes the ability to further refine or constrain filtering criteria to either display a greater or lesser number of plan	S	

Small Business Requirements Traceability Matrix

SH-13	Small Business	Plan Selection	OneGate	OneGate	Provide capability for an employer to select QHP(s), or a tier, and initiate the participation process.	S	
SH-14	Small Business	Plan Selection	OneGate	OneGate	Provide functionality to have a small business tax calculator available to small employers.	S	

Small Business Requirements Traceability Matrix

SH-15	Small Business	Plan Selection	OneGate	OneGate	Once a plan, plans or a tier is selected, direct an employer to instructions on payment remittance for monthly premiums and coordinating the benefit election process with employees.	W	
SH-16	Small Business	Plan Selection	OneGate	OneGate	If applicable, display an adjusted plan final cost based on small business tax credit eligibility, enumerating the costs prior to the small business tax credit, the projected savings for the employer from the small business tax credit and the final costs to the employer	S	

Small Business Requirements Traceability Matrix

SH-17	Small Business	Plan Selection	OneGate	OneGate	For informational purposes only, provide ability to generate on-screen notification to employers who select a Small Business Tax Credit of the possibility of tax penalties / liabilities at time of tax filing should their business size or income change.	W	
SH-18	Small Business	Plan Selection	OneGate	OneGate	Provide an online calculator for an employer to estimate potential eligibility as well as potential tax credit under the 4 tiers of qualified health plan benefits.	S	

Small Business Requirements Traceability Matrix

SH-19	Small Business	Employer/Employee Application	OneGate	OneGate	Provide capability to accept paper documents for SHOP, such as employer / employee applications and verifications.	W	
SH-20	Small Business	Employer Application	OneGate	OneGate	Allow verified individuals to complete employer applications on behalf of the employer (i.e. an administration or finance department/personnel, etc.)	S	

Small Business Requirements Traceability Matrix

SH-21	Small Business	Employer Application	OneGate	OneGate	Provide a single, online employer application for Small Business	S	
SH-22	Small Business	Employer Application	OneGate	OneGate	During the Application Process, prompt the Employer to enter the exact business name associated with the EIN.	S	

Small Business Requirements Traceability Matrix

SH-23	Small Business	Employer Application	OneGate	OneGate	Provide the capability to differentiate / track full-time employees versus part-time/hourly employees in the employee roster.	S	
SH-24	Small Business	Employer Application	OneGate	OneGate	Validate field-level information for correct data format and completeness	S	

Small Business Requirements Traceability Matrix

SH-25	Small Business	Employer Application	Loqate	Loqate	Conduct validation of mailing addresses provided in applications (using external Postal Address validation service)	S	
SH-26	Small Business	Employer Application	OneGate	OneGate	For employers who do not have an EIN, allow the application process to proceed (e.g. businesses in the process of obtaining an EIN, etc.) Per the 30-day validation process, allow for the suspense of eligibility if EIN remains un-verified.	W	

Small Business Requirements Traceability Matrix

SH-27	Small Business	Employer/Employee Application	OneGate	OneGate	Within the employer and employee application, the Exchange shall validate field-level information for format and completeness	S	
SH-28	Small Business	Employer Application	OneGate	OneGate	Provide capability to utilize / create a single client identifier for the Exchange and use that identifier to locate the employer at the point of application / account creation / renewals, etc., as applicable.	S	

Small Business Requirements Traceability Matrix

SH-29	Small Business	Employer Application	OneGate	OneGate	Prior to the creation of a new employer account, the Exchange shall determine if an existing user account is present based on matching criteria provided in the application (e.g. EIN, name)	S	
SH-30	Small Business	Employer Application	N/A	N/A	Provide capability to validate employee SSNs submitted through the employer application (employee roster).	**N/A**	In accordance with RFP Amendment 2 Question 171, this requirement is deleted

Small Business Requirements Traceability Matrix

SH-31	Small Business	Employer Application	Oracle Identity Manager	Oracle Identity Manager	Create user name and password for each employee listed on employee roster.	W	
SH-32	Small Business	Employer Application	OneGate	OneGate	Allow employer-authorized broker/assister to submit all or select data for Employer Application	S	

Small Business Requirements Traceability Matrix

SH-33	Small Business	Employer Application	OneGate	OneGate	Capture broker/assister of record in the employer and account information	S	
SH-34	Small Business	Employer/Employee Application	OneGate	OneGate	At the point when an employer builds an initial employee roster, the SHOP Exchange will not need to establish unique individual identifiers utilizing the eligibility and enrollment database. However, when employees utilize the exchange after notification from their employers, the	C	CGI will build interfaces between OneGate and the Identity Management Solution to provide this capability.

Small Business Requirements Traceability Matrix

SH-35	Small Business	Employer/Employee Application	OneGate	OneGate	During the application process, user accounts shall be created that include the following: - User unique identifier - User demographic information - Application status - Participation status - Existing program eligibility (Small Business	S	
SH-36	Small Business	Employer/Employee Application	OneGate	OneGate	Support the creation of a user account for both employers and employees that defines a user-defined, user name and password.	S	

Small Business Requirements Traceability Matrix

SH-37	Small Business	Plan Selection	OneGate	OneGate	Update an employer's account to reflect plan selection and the effective projected plan-year.	S	
SH-38	Small Business	Communicate Options to Employees	OneGate	OneGate	Provide the capability for the employer to generate a packet of critical information to distribute to the employee.	W	

Small Business Requirements Traceability Matrix

SH-39	Small Business	Communicate Options to Employees	OneGate	OneGate	Upon submittal of initial Employer Application, provide email or written notification to employees (as identified on the employee roster) to elect for or opt-out of employer sponsored coverage. Notification should also provide instructions and information to the	W	
SH-40	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide capability to generate a request to the DLIR to verify an employer's size. (e.g. using EIN, HBI, actual payroll, Master Business License Application, income tax documents, etc.)	W	

Small Business Requirements Traceability Matrix

SH-41	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide the capability to initiate a manual verification process when additional verification of employer size is required. (e.g. using EIN, HBI, actual payroll, Master Business License Application, income tax documents, etc.)	F	This functionality will be included in the April 2013 release
SH-42	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Display the result of the verification provided by DLIR; provide means for an employer to dispute, call into question or appeal the validity of data from authoritative sources	F	This functionality will be included in the April 2013 release

Small Business Requirements Traceability Matrix

SH-43	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide capability to electronically store documents submitted for verification of employer size, business address, coverage, and number of full-time employees.	S	
SH-44	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Track status of employer size verification based on the following: - Verified - Not verified - Pending Review	S	

Small Business Requirements Traceability Matrix

SH-45	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide capability to produce a mailed, written notice to the employer to provide additional verifications (notices are sent out nightly in batch); the automated written notice shall include: - Employer name - Address - Unique identifier,	W	
SH-46	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	When additional verification is required, provide on-screen notification to employer to supply additional verifications through the Exchange.	S	

Small Business Requirements Traceability Matrix

SH-47	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Update user / employer account status based on updated results for employer size, business address, coverage and number of full time employees	W	
SH-48	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide capability to generate a request to the Information Source To Be Determined (TBD) to verify Business Address or Worksite.	W	

Small Business Requirements Traceability Matrix

SH-49	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide the capability to initiate a manual verification process when additional verification of Business Address or Worksite is required.	W	
SH-50	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Display the result of the verification provided by Information Source TBD; provide means for an employer to dispute, call into question or appeal the validity of data from authoritative sources	C	CGI will build the interfaces between OneGate and designated information sources.

Small Business Requirements Traceability Matrix

SH-51	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide capability to electronically store documents submitted for Business Address or Worksite verification.	S	
SH-52	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Track status of verification separately for employer size, business address, coverage and number of full time employees based on the following: - Verified - Not verified - Pending Review	S	

Small Business Requirements Traceability Matrix

SH-53	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Produce a mailed, written notice to the employer to provide additional verifications (notices are sent out nightly in batch); the automated written notice shall include: - Employer name - Address - Unique identifier, potentially	W	
SH-54	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	When additional verification is required, provide on-screen notification to employer to supply additional verifications through the Exchange.	S	

Small Business Requirements Traceability Matrix

SH-55	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide capability to generate a request to the Information Source To Be Determined (TBD) to verify Coverage Offered to all Full Time Employed Employees, if applicable.	W	
SH-56	Small Business	Verify Employer Data on Eligibility Application	OneGate	OneGate	Provide the capability to initiate a manual verification process when additional verification of Coverage Offered to all Full Time Employed Employees is required.	W	

Small Business Requirements Traceability Matrix

SH-57	Small Business	Determine Employer Eligibility	OneGate	OneGate	Provide capability to allow employer participation upon initial application, but to terminate participation if original eligibility information is in question and is not substantiated within thirty days.	W	
SH-58	Small Business	Determine Employer Eligibility	OneGate	OneGate	Generate a request to determine whether an employer meets size, location and employee coverage requirements to utilize the Small Business Exchange	S	

Small Business Requirements Traceability Matrix

SH-59	Small Business	Determine Employer Eligibility	OneGate	OneGate	Conduct an eligibility determination as to whether an employer meets size, location and employee coverage requirements to utilize the Small Business Exchange	S	
SH-60	Small Business	Determine Employer Eligibility	OneGate	OneGate	Based on size, location and employee coverage, determine whether an employer is eligible to select and participate in a QHP through the Small Business Exchange.	S	

Small Business Requirements Traceability Matrix

SH-61	Small Business	Determine Employer Eligibility	OneGate	OneGate	Generate written and on-screen notification of the result of an employer's eligibility determination	S	
SH-62	Small Business	Plan Selection	OneGate	OneGate	Allow the Exchange to set different start dates and waiting periods for different QHPs and employers	W	

Small Business Requirements Traceability Matrix

SH-63	Small Business	Plan Selection	OneGate	OneGate	Prevent employers that have current QHP selection(s) pending from adding new QHP(s) or changing their pending selection.	W	
SH-64	Small Business	Plan Selection / Employee Enrollment	Healthation	Healthation	After plan selection by the employees and the employer has re-evaluated their plan costs and submitted payment, initiate the plan enrollment process / transaction to applicable carriers.	S	

Small Business Requirements Traceability Matrix

SH-65	Small Business	Employer Contribution	OneGate	OneGate	Provide the capability to determine participation rates of an employer's employees. Provide the capability to share this information with issuers.	S	
SH-66	Small Business	Employer Contribution	OneGate	OneGate	Once plan costs are finalized along with the Employee Census, provide onscreen and written notification to the employer, with summary and detailed cost information.	W	

Small Business Requirements Traceability Matrix

SH-67	Small Business	Employer Contribution	OneGate	OneGate	Following the enrollment of an employer's employees selecting plan(s) for themselves and any dependents, the employer shall have the capability to view and confirm the costs imparted upon the employer.	S	Need to determine if employer payment is a prerequisite for employee enrollment
SH-68	Small Business	Employer Contribution	OneGate	OneGate	When plan costs to the employer are finalized, the Small Business Exchange shall provide the flexibility for the Employer to review and compare alternative plans.	S	

Small Business Requirements Traceability Matrix

SH-69	Small Business	Employer Contribution	OneGate	OneGate	Allow configuration for setting up different types of employer contributions such as percentage of the cost, a dollar value, metal levels, or other options	S	
SH-70	Small Business	Employer Contribution	OneGate	OneGate	Provide decision support tools, including an online calculator that supports 'what if' scenarios	S	

Small Business Requirements Traceability Matrix

SH-71	Small Business	Employer Contribution	OneGate	OneGate	Recognize future coverage, and manage the effective date based on future coverage information	F	Will be part of the April 2013 release
SH-72	Small Business	Employer Contribution	OneGate	OneGate	Allow employer contribution to be based on multiple employee choice models, including choice within a tier, choice within a carrier, or full employee choice	S	

Small Business Requirements Traceability Matrix

SH-73	Small Business	Employer Contribution	OneGate	OneGate	Allow employers to provide a contribution for employees to select a plan on the Individual Exchange	F	Will be part of the April 2013 release
SH-74	Small Business	Employer Contribution	OneGate	OneGate	Allow employers to use wage information to compare coverage options to alternatives available to their employees in the Individual Exchange	F	Will be part of the April 2013 release

Small Business Requirements Traceability Matrix

SH-75	Small Business	Plan Selection / Employee Enrollment	Healthation	Healthation	Upon acceptance of final offer from carrier to employer and collection of 1st month's premium payment, generate enrollment transaction to a carrier.	S	
SH-76	Small Business	Employer / Employee Termination	OneGate	OneGate	Provide capability to provide termination notices in multiple forms, including in email and paper form.	W	

Small Business Requirements Traceability Matrix

SH-77	Small Business	Employer / Employee Termination	OneGate	OneGate	Allow SHOP Employers to identify/manage the employees within the Exchange	S	
SH-78	Small Business	Employer Termination	OneGate	OneGate	Provide capability to provide notifications (i.e. termination notice, billing notices) as imaged documents during the employer's activities and for the employer to be able to view at a later date.	W	

Small Business Requirements Traceability Matrix

SH-79	Small Business	Employer Termination	OneGate	OneGate	Provide capability to administer COBRA, supporting these enrollments and disenrollments.	W	Our solution will display COBRA plans assuming they are provided in a format which can be stored in Plan Management and that no unique processing rules apply.
SH-80	Small Business	Employer Termination	OneGate	OneGate	Provide the capability for an employer to request a voluntary termination from QHP(s) at any time.	S	

Small Business Requirements Traceability Matrix

SH-81	Small Business	Employer / Employee Termination	OneGate	OneGate	If an employer initiates a voluntary termination through the Exchange, produce an electronic notification to the employer's employees to inform them of the employer termination. The notice should contain information relating an appeals process and other	W	
SH-82	Small Business	Employer Termination	OneGate	OneGate	If an employer initiates a voluntary termination, produce an electronic notification to the Issuer to terminate the employer.	W	

Small Business Requirements Traceability Matrix

SH-83	Small Business	Employer Termination	OneGate	OneGate	If conditions for a voluntary termination, initiate the employer termination process.	W	
SH-84	Small Business	Employer Termination	OneGate	OneGate	Provide the capability to image and store documents sent to the employer regarding the employer's termination.	W	

Small Business Requirements Traceability Matrix

SH-85	Small Business	Employer / Employee Termination	OneGate	OneGate	Update user accounts based on termination notification from issuers or terminations initiated by the Exchange.	W	
SH-86	Small Business	Employer Termination	OneGate	OneGate	Prepare a notice to CMS with a minimum dataset of information regarding an employer's voluntary termination from a qualified health plan through the Exchange. This information may be used for small business tax credits, as well as for individual mandates, etc.,	F	OneGate will provide an unconfigured trigger to the notifications solution to generate notifications. OneGate will also pass in the necessary data to the notifications solution to generate notifications. This will be available in the April 2013 release.

Small Business Requirements Traceability Matrix

SH-87	Small Business	Employer Termination	OneGate	OneGate	Provide capability to receive electronic notifications from issuers regarding involuntary terminations and initiate termination process.	W	
SH-88	Small Business	Employer Termination	OneGate	OneGate	If an employer has an involuntary termination through the Exchange, produce an electronic notification to the employer to inform the employer of the employer termination.	W	

Small Business Requirements Traceability Matrix

SH-89	Small Business	Employer Termination	OneGate	OneGate	Provide capability to produce two different notifications to employees during a involuntary employer termination, regarding the potential or actual termination of an employer.	W	
SH-90	Small Business	Employer Termination	OneGate	OneGate	If conditions for an involuntary termination are present, initiate the termination process.	W	

Small Business Requirements Traceability Matrix

SH-91	Small Business	Employer Termination	OneGate	OneGate	If an employer has an involuntary termination through the Exchange, prepare communication to the Issuer to terminate the employer.	W	
SH-92	Small Business	Employer Termination	OneGate	OneGate	Update user accounts based on termination notification from issuers or terminations initiated by the Exchange.	W	

Small Business Requirements Traceability Matrix

SH-93	Small Business	Employer Termination	OneGate	OneGate	Prepare a notice to CMS with a minimum dataset of information regarding an employer's involuntary termination from a qualified health plan through the Exchange. This information may be used for small business tax credits, as well as for individual mandates, etc.,	F	OneGate will provide an unconfigured trigger to the notifications solution to generate notifications. OneGate will also pass in the necessary data to the notifications solution to generate notifications. This will be available in the April 2013 release.
SH-94	Small Business	Employer Termination	OneGate	OneGate	Notify QHPs when an employer terminates coverage and ensure coverage is discontinued	W	

mall Business Requirements Traceability Matrix

SH-95	Small Business	Employer Termination	OneGate	OneGate	Notify employees when an employer terminates coverage and ensure coverage is discontinued. Employees must be given a 30 day notice of termination.	W	
SH-96	Small Business	Renewal	OneGate	OneGate	Provide capability for employers to submit changes to key eligibility factors for the purpose of annual eligibility / participation renewal. Supported methods of reporting changes include written forms and web-based responses through the Exchange.	S	

Small Business Requirements Traceability Matrix

SH-97	Small Business	Renewal	OneGate	OneGate	Process employer responses to renew eligibility and initiate eligibility determination process if necessary. The Exchange shall review employer Exchange eligibility and shall have the capability to review small business tax credit eligibility. The Exchange	S	
SH-98	Small Business	Renewal	OneGate	OneGate	Provide the capability to calculate a year-to-date average for premiums paid and monthly income for display to the employer at time of renewal.	W	

Small Business Requirements Traceability Matrix

SH-99	Small Business	Employer Renewal	OneGate	OneGate	Based on the availability of QHP(s), determine availability of an employer's current plan for the purposes of participation renewal.	S	
SH-100	Small Business	Employer Renewal	OneGate	OneGate	If the employer's current plan(s) are no longer available, provide capability to automatically suggest employer participation for a default health plan(s) for a geographic area.	F	This functionality will be available in the April 2013

Small Business Requirements Traceability Matrix

SH-101	Small Business	Update Employer Eligibility Application	OneGate	OneGate	Provide capability for employers to submit changes to SHOP plan participation (selected plan(s), selected tier (optional), covered employers, etc.). Supported methods of enrollment changes include written forms and web-based responses	S	
SH-102	Small Business	Renewal, Employee Enrollment	OneGate	OneGate	Based on an employer's responses to enrollment renewal, assess responses for need to initiate enrollment into a new QHP or additional employers into an existing QHP.	S	

Small Business Requirements Traceability Matrix

SH-103	Small Business	Renewal, Employee Enrollment	OneGate	OneGate	Based on an employer's responses to enrollment renewal, process enrollment selections if possible.	S	
SH-104	Small Business	Renewal, Employee Enrollment	OneGate	OneGate	Process notification notifying employer of coverage for employees. Also, communicate any next steps required by the employer.	S	

Small Business Requirements Traceability Matrix

SH-105	Small Business	Employer Renewal	OneGate	OneGate	Process employer renewal in a method very similar to the initial employer application, allowing for the submission of an updated employee roster, processing plan selection options based on preferences, and submitting notifications to the employer.	S	
SH-106	Small Business	Update Employer Eligibility Application	OneGate	OneGate	Based on employer status, determine eligibility for SHOP participation renewal (e.g. annual renewal).	S	

Small Business Requirements Traceability Matrix

SH-107	Small Business	Update Employer Eligibility Application	OneGate	OneGate	Produce written notification / request for employers to verify key eligibility factors (continue to has a current EIN, etc.) for the purposes of annual eligibility / participation renewal and report changes if necessary.	W	
SH-108	Small Business	Employer Renewal	OneGate	OneGate	Produce a notice of annual open enrollment.	W	

Small Business Requirements Traceability Matrix

SH-109	Small Business	Employer Renewal	OneGate	OneGate	Present opportunity for employer to log-in to initiate their renewal.	S	
SH-110	Small Business	Appeal Small Business Eligibility Decision	OneGate	OneGate	In all notices produced by the Exchange regarding eligibility determination, notify employers to their rights and responsibilities (including a right to appeal eligibility decisions).	W	

mall Business Requirements Traceability Matrix

SH-111	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability to capture information and details of a Employer complaint.	S	
SH-112	Small Business	Appeal Small Business Eligibility Decision	OneGate	OneGate	Allow employers to review record of participation in the Small Business Exchange.	S	

Small Business Requirements Traceability Matrix

SH-113	Small Business	Appeal Small Business Eligibility Decision	OneGate	OneGate	Provide the flexibility to extend interim coverage or manage disenrollments based on events such as: - Flexible grace periods during enrollments and disenrollments (including during appeals process where final eligibility determination is not confirmed)	W	
SH-114	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability for an employer to request an appeal to the employer eligibility decision.	S	

mall Business Requirements Traceability Matrix

SH-115	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability to differentiate between appeals and complaints; default requests to complaints when received by employers unless specifically indicated as an appeal.	S	
SH-116	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability to capture, track, and disposition appeals in the Exchange (including status, assignments, and relevant case notes).	S	

Small Business Requirements Traceability Matrix

SH-117	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability to refer or route appeal requests to entities outside of the Exchange such as an Independent Review Organization or Issuers.	W	
SH-118	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide capability for an employer to view key employer account information (includes employer details as well as key eligibility factors used to determine eligibility).	S	

Small Business Requirements Traceability Matrix

SH-119	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide the capability to record the detailed results and supporting documentation that result from or support an appeals decision.	W	
SH-120	Small Business	Appeal Small Business Eligibility Decision	OneGate	OneGate	Generate a formal written notice informing an employer of the details of an appeal decision.	W	

Small Business Requirements Traceability Matrix

SH-121	Small Business	Appeal Small Business Eligibility Decision	OneGate	OneGate	Allow employers to request and receive a second appeal review process, providing very similar, if not the same, steps in the second appeal process as the first appeal process.	W	
SH-122	Small Business	Appeal Small Business Eligibility Decision	OneGate	OneGate	Generate a notification to CMS of appeals decisions in which a renewal is denied.	W	

Small Business Requirements Traceability Matrix

SH-123	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Provide capability for employers to submit changes to employee roster (add / remove employees) in between redeterminations / renewals.	S	
SH-124	Small Business	Change Reporting	OneGate	OneGate	Provide the capability for employers to submit changes to the employee rosters, using multiple methods (i.e. submission of files, completion of data fields, etc.)	S	

Small Business Requirements Traceability Matrix

SH-125	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Upon reporting changes in offers of coverage to all Full Time Employees re-evaluate eligibility for participation in Small Business.	S	
SH-126	Small Business	Periodic Reporting and Reconciliation	OneGate	OneGate	Prepare and send communication to the employer regarding changes to the employer's employee roster.	W	

Small Business Requirements Traceability Matrix

SH-127	Small Business	Change Reporting/Periodic Reporting	OneGate	OneGate	Provide capability for employers to check the status of employee QHP enrollment through the web portal.	S	
SH-128	Small Business	Change Reporting/Periodic Reporting	OneGate	OneGate	Provide capability to prepare and send information-only communication to the employer regarding potential changes to their Tax Credit Eligibility due to a change in the employee roster. Provide a link to IRS website for additional information regarding the	S	

Small Business Requirements Traceability Matrix

SH-129	Small Business	Change Reporting/Periodic Reporting	OneGate	OneGate	Provide the capability to recalculate the employer's total cost based on reported changes to the employee roster.	S	
SH-130	Small Business	Update Employee Application	OneGate	OneGate	Provide the capability for employers to submit changes to the employer contact information.	S	

Small Business Requirements Traceability Matrix

SH-131	Small Business	Update Employee Application	Healthation	Healthation	Report employer contact information changes to the Issuer.	W	
SH-132	Small Business	Update Employee Application	OneGate	OneGate	Prepare and send communication to the employer regarding changes to the Employer contact information.	W	

Small Business Requirements Traceability Matrix

SH-133	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Initiate the termination process if the employer is to be found no longer eligible for the Exchange.	W	
SH-134	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Provide the capability for employers to submit changes about the employer's principal business address or primary worksite location.	S	

Small Business Requirements Traceability Matrix

SH-135	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Provide the ability to capture a reported change in the employer's principal business location and satellite offices.	W	
SH-136	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Provide notification to employers when annual election period is approaching	W	

Small Business Requirements Traceability Matrix

SH-137	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Provide an immediate message to the employer warning about likely termination if they provide a primary worksite location or principal business address that is outside of the state.	S	Need requirements to determine threshold of "in state" criteria
SH-138	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Provide the capability to determine employer eligibility based on the employer's principal business location and satellite offices.	W	

mall Business Requirements Traceability Matrix

SH-139	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Provide the capability to re-evaluate an employer's eligibility for Small Business when a change is made to the employer's work location or satellite offices.	W	
SH-140	Small Business	Renew / Redetermine Employer Participation	OneGate	OneGate	Prepare and send communication to the employer regarding changes to the Employer's worksite locations.	S	

Small Business Requirements Traceability Matrix

SH-141	Small Business	Renew/Redetermine Employer Participation	OneGate	OneGate	Brokers / Employer Agents shall have the ability to enter information and be provided services in a manner identical or very similar to that of the employer's.	S	
SH-142	Small Business	Prepare Employee Application	OneGate	OneGate	Provide the capability to identify Employers (or Employer's representatives like Human Resources, Administrative staff, etc.) if the Employers or Representatives are completing applications on behalf of an employee. Also, provide the capability for employers to update	W	

Small Business Requirements Traceability Matrix

SH-143	Small Business	Prepare Employee Application	OneGate	OneGate	To confirm Small Business eligibility, first request that employee log-in with user name and password.	S	
SH-144	Small Business	Prepare Employee Application	Oracle Identity Manager	Oracle Identity Manager	Prompt employees to update all account information, including the password upon initial log in.	S	

Small Business Requirements Traceability Matrix

SH-145	Small Business	Verify Employee Application Data	OneGate	OneGate	Conduct a validation of SSN provided versus the name provided (i.e. validate against name on record with Social Security Administration database). Track any validations made.	W	
SH-146	Small Business	Verify Employee Application Data	OneGate	OneGate	Provide capability to verify if employee exists on employee roster in order to verify an employee's coverage through an employer.	S	

mall Business Requirements Traceability Matrix

SH-147	Small Business	Verify Employee Application Data	OneGate	OneGate	Display the result of the verification process.	S	
SH-148	Small Business	Determine Employee Eligibility	OneGate	OneGate	Update user /employee account status based on updated employee coverage results	F	This functionality will be available in the April 2013

Small Business Requirements Traceability Matrix

SH-149	Small Business	Determine Employee Eligibility	OneGate	OneGate	Provide the capability to track the response / status of employees who have been offered employer-sponsored coverage. Key statuses to track include waiver of coverage / elected for coverage / non-participation.	S	
SH-150	Small Business	Determine Employee Eligibility	OneGate	OneGate	Inform employees that may be eligible for subsidized coverage at a lower premium and allow for an individual eligibility determination.	S	There is not a regulatory restriction - but we will research

mall Business Requirements Traceability Matrix

SH-151	Small Business	Prepare Employee Application	OneGate	OneGate	Present an initial set of screening questions in the initial employee application process to identify the following applicant characteristics: - Employee name - Employee Address - Social security number - Other Employee Contact Information	S	
SH-152	Small Business	Prepare Employee Application	OneGate	OneGate	Provide the capability to use the model single employee application provided by HHS.	S	

Small Business Requirements Traceability Matrix

SH-153	Small Business	Prepare Employee Application	OneGate	OneGate	Provide additional language support in accordance with Exchange language support guidlines.	S	
SH-154	Small Business	Prepare Employee Application	OneGate	OneGate	Provide field level help for each application data element that includes description and required data format.	S	

mall Business Requirements Traceability Matrix

SH-155	Small Business	Prepare Employee Application	OneGate	OneGate	Provide capability for employees to access in-depth online help during the application process.	S	
SH-156	Small Business	Prepare Employee Application	Siebel Public Sector CRM	Siebel Public Sector CRM	Provide capability for employees to request further assistance through Chat Support (online assistance from a customer service representative) during the application process.	W	

Small Business Requirements Traceability Matrix

SH-157	Small Business	Prepare Employee Application	OneGate	OneGate	During the Application Process, prompt the Employee to enter the exact name associated with the SSN.	S	
SH-158	Small Business	Prepare Employee Application	OneGate	OneGate	If an application is initiated by a Navigator, the Exchange shall have the capability for the employee to attest that the information provided by the Navigator is accurate.	S	

nall Business Requirements Traceability Matrix

H-159	Small Business	Prepare Employee Application	OneGate	OneGate	Provide the capability to identify Navigators (or Brokers, etc.) if they are completing applications on behalf of an employee.	S	
H-160	Small Business	Prepare Employee Application	OneGate	OneGate	Accept paper documents for SHOP, including employee applications.	S	

Small Business Requirements Traceability Matrix

SH-161	Small Business	Prepare Employee Application	OneGate	OneGate	Validate field-level information for correct data format and completeness.	S	
SH-162	Small Business	Prepare Employee Application	Loqate	Loqate	Conduct validation of mailing addresses provided in applications (using external Postal Address validation service).	S	

mall Business Requirements Traceability Matrix

H-163	Small Business	Prepare Employee Application	OneGate	OneGate	Conduct a validation of SSN provided versus the employee name provided (i.e. validate against name on record with SSN database) and provide capability to validate SSN versus other criteria.	W	
H-164	Small Business	Prepare Employee Application	OneGate	OneGate	For employees who do not have a SSN, allow the application process to proceed.	S	

Small Business Requirements Traceability Matrix

SH-165	Small Business	Prepare Employee Application	OneGate	OneGate	Within the QHP application, the Exchange shall validate field-level information for format and completeness.	S	
SH-166	Small Business	Prepare Employee Application	OneGate	OneGate	During the application process, user accounts shall be created that include the following, and will be linked to the following information in the Employee Roster: - Employee Names and Employee SSN - Employer EIN	S	

mall Business Requirements Traceability Matrix

SH-167	Small Business	Prepare Employee Application	OneGate	OneGate	Save application information to user account after account creation.	S	
SH-168	Small Business	Prepare Employee Application	Oracle Identity Manager	Oracle Identity Manager	Prior to the creation of a new user account, the Exchange shall determine if an existing user account is present based on matching criteria provided in the application (e.g. SSN, name, identifying questions)	W	

Small Business Requirements Traceability Matrix

SH-169	Small Business	Prepare Employee Application	Oracle MDM (Customer Hub)	Oracle MDM (Customer Hub)	If consumers can be enrolled in Medicaid and Small Business simultaneously, a consumers' unique identifier shall indicate this dual enrollment for any consumers that are enrolled in both Medicaid and Small Business.	W	
SH-170	Small Business	Prepare Employee Application	OneGate	OneGate	During the application process, user accounts shall allow for the inclusion of the following: - User unique identifier - User demographic information - Application status - Enrollment status	S	

mall Business Requirements Traceability Matrix

H-171	Small Business	Employee Selects QHP	OneGate	OneGate	Generate a request to initiate the employee selection of qualified health plan after eligibility determination is verified or if employee participation is allowed pending verification of eligibility information.	S	
H-172	Small Business	Employee Selects QHP	OneGate	OneGate	Produce a real-time electronic request to the employee to determine employee preferences for qualified health plan(s).	S	

Small Business Requirements Traceability Matrix

SH-173	Small Business	Employee Selects QHP	OneGate	OneGate	Allow employee to enter information about employee dependents, if employers are choosing to provide coverage to employees' dependents. Dependent information gathered will include, but is not limited to the following: - Name	S	
SH-174	Small Business	Verify Indian Status	OneGate	OneGate	Provide capability to validate employee Indian status of employee and/or dependent(s) submitted through the employee application.	W	

nall Business Requirements Traceability Matrix

H-175	Small Business	Plan Selection	OneGate	OneGate	Based on carrier and plan information gathered, display plan cost and availability.	S	
H-176	Small Business	Employee Selects QHP	OneGate	OneGate	As a default, only display health plans that have been selected by the employer, are certified by the Exchange, are open to additional enrollment, and are available in the employee's geographic area.	S	

Small Business Requirements Traceability Matrix

SH-177	Small Business	Employee Selects QHP	OneGate	OneGate	Display projected actual plan cost (net premium) based on employer groups and applicable rating factors (consumers covered, age, geography, quality ratings, etc.) to the employee during the application process.	S	
SH-178	Small Business	Employee Selects QHP	OneGate	OneGate	Provide capability to display a detailed comparison of available employer-selected health plans based on employee preferences	S	

mall Business Requirements Traceability Matrix

SH-179	Small Business	Employee Selects QHP	OneGate	OneGate	Store enrollment questionnaire responses and display plan choices based on application / filtering criteria.	S	
SH-180	Small Business	Employee Selects QHP	OneGate	OneGate	Provide capability to view and select plan(s) for employee dependents, if covered by employer	S	

Small Business Requirements Traceability Matrix

SH-181	Small Business	Employee Selects QHP	OneGate	OneGate	Grant access to an updated provider directory for employee plan selection. This directory should be current at the point in time in which the employer accesses the directory.	S	
SH-182	Small Business	Employee Selects QHP	OneGate	OneGate	Provide capability for employees to adjust employee preferences and update display / comparison of available qualified health plans. This capability includes the ability to further refine or constrain filtering criteria to either display a greater or lesser number of plan	S	

mall Business Requirements Traceability Matrix

H-183	Small Business	Employee Selects QHP	OneGate	OneGate	Provide information and provide capability to allow employees determine if their premium costs are such that the costs make the employee eligible for purchasing insurance through the individual market or allow the employee to be exempt from the individual	S	
H-184	Small Business	Employee Selects QHP	OneGate	OneGate	Allow employees to have a choice of Exchange's competing plans, based on employer selections and (given the employer contribution) see what their contribution requirement would be for each choice	S	

Small Business Requirements Traceability Matrix

SH-185	Small Business	Employee Selects QHP	OneGate	OneGate	Provide capability for an employee to select QHP(s) and initiate the enrollment process.	S	
SH-186	Small Business	Employee Selects QHP	OneGate	OneGate	Update an employee's account to reflect plan selection and the effective projected plan-year.	S	

nall Business Requirements Traceability Matrix

H-187	Small Business	Employee Selects QHP	Healthation	Healthation	After plan selection, initiate the financial transactions required by employers to ensure plan enrollment process / transaction to applicable carriers.	W	
H-188	Small Business	Employee Selects QHP	OneGate	OneGate	After acknowledgement of the receipt of the plan selection, initiate the calculation of the final cost to employee	S	

Small Business Requirements Traceability Matrix

SH-189	Small Business	Employee Selects QHP	OneGate	OneGate	After acknowledgement of the receipt of the plan selection, display the calculation of the final cost (net premium) to employee	S	
SH-190	Small Business	Employee Selects QHP	OneGate	OneGate	Provide a reminder that an employee receives tax relief when the employee purchases health insurance via their employer at through a pre-tax payroll deduction.	W	

mall Business Requirements Traceability Matrix

H-191	Small Business	Employee Selects QHP	OneGate	OneGate	Produce an automated and real-time, electronic notification of plan selection.	W	
H-192	Small Business	Employee Selects QHP	OneGate	OneGate	Provide the capability to verify and acknowledge the receipt of the plan selection.	S	

Small Business Requirements Traceability Matrix

SH-193	Small Business	Employee Selects QHP	OneGate	OneGate	Upon employee's QHP selection, notify the employer of it own and each employee's respective contribution amount in order to facilitate appropriate payroll deductions as needed	W	
SH-194	Small Business	Employee Enrollment in QHP	OneGate	OneGate	Prepare a communication to Issuer regarding employee enrollment in QHP	W	

mall Business Requirements Traceability Matrix

SH-195	Small Business	Employee Enrollment in QHP	Healthation	Thru Premium Processor / not CGI	Receive and process acknowledgement of employee enrollment from Issuer	W	
SH-196	Small Business	Employee Enrollment in QHP	OneGate	OneGate	Provide notification of successful enrollment to employee	W	

Small Business Requirements Traceability Matrix

SH-197	Small Business	Employee Enrollment in QHP	OneGate	OneGate	Provide notification to CMS regarding employee enrollment	W	
SH-198	Small Business	Update Employee Eligibility Application	OneGate	OneGate	Allow employees to enroll in QHP during a qualifying event.	S	

nall Business Requirements Traceability Matrix

H-199	Small Business	Disenroll Employee in QHP	OneGate	OneGate	Provide the capability for an employee to request a voluntary disenrollment from QHP(s).	S	
H-200	Small Business	Disenroll Employee in QHP	OneGate	OneGate	If an employee initiates a voluntary disenrollment through the Exchange, produce an electronic notification to the employee's employer to inform them of the employee disenrollment.	W	

mall Business Requirements Traceability Matrix

SH-201	Small Business	Disenroll Employee in QHP	OneGate	OneGate	If an employee initiates a voluntary disenrollment through the Exchange, produce an electronic notification to the Issuer to disenroll the employee.	W	
SH-202	Small Business	Disenroll Employee in QHP	OneGate	OneGate	Provide capability to initiate the disenrollment process.	S	

mall Business Requirements Traceability Matrix

H-203	Small Business	Disenroll Employee in QHP	OneGate	OneGate	Provide capability to update user accounts based on disenrollment notification from issuers	S	
H-204	Small Business	Disenroll Employee in QHP	OneGate	OneGate	Update user accounts based on disenrollment notification from disenrollment initiated by the Exchange.	S	

Small Business Requirements Traceability Matrix

SH-205	Small Business	Disenroll Employee in QHP	OneGate	OneGate	Prepare a notice to CMS with a minimum dataset of information regarding an employee's disenrollment from a qualified health plan through the Exchange. This information is used for tax administration, as applicable.	W	
SH-206	Small Business	Disenroll Employee in QHP	Healthation	??	Provide capability to receive electronic notifications from Issuers regarding disenrollment and initiate disenrollment process.	W	

mall Business Requirements Traceability Matrix

H-207	Small Business	Disenroll Employee in QHP	OneGate	OneGate	If an employee has a disenrollment through the Exchange, produce an electronic notification to the employee's employer to inform them of the employee termination and alternative insurance options.	W	
H-208	Small Business	Disenroll Employee in QHP	OneGate	OneGate	If an employee has an involuntary disenrollment through the Exchange, produce an electronic notification to the employee to inform the employee of the employee disenrollment.	W	

Small Business Requirements Traceability Matrix

SH-209	Small Business	Disenroll Employee in QHP	OneGate	OneGate	If conditions for an involuntary disenrollment, initiate the disenrollment process.	W	
SH-210	Small Business	Disenroll Employee in QHP	OneGate	OneGate	If an employee has an involuntary disenrollment through the Exchange, prepare communication to the Issuer to terminate the employee.	W	

mall Business Requirements Traceability Matrix

H-211	Small Business	Disenroll Employee in QHP	OneGate	OneGate	Update user accounts based on disenrollment notification from issuers or disenrollment initiated by the Exchange.	W	
H-212	Small Business	Disenroll Employee in QHP	OneGate	OneGate	Prepare a notice to CMS with a minimum dataset of information regarding an employee's termination from a qualified health plan through the Exchange. This information is used for tax administration, etc., as applicable.	W	

Small Business Requirements Traceability Matrix

SH-213	Small Business	Renew Employee QHP Participation	OneGate	OneGate	Provide automatic renewal notice to employees	W	
SH-214	Small Business	Update Employee Application / Renew Employee QHP Participation	Oracle Identity Manager	Oracle Identity Manager	If an employee does not have their log-in information (User name and/or password) available to them for plan renewal, present opportunity for the employee to request their log-in information. The log-in information may be emailed to the employee after their	W	

nall Business Requirements Traceability Matrix

H-215	Small Business	Renew Employee QHP Participation	OneGate	OneGate	Track annual renewal date for employers.	S	
H-216	Small Business	Update Employee Application / Renew Employee QHP Participation	OneGate	OneGate	Based on employee status, determine eligibility for SHOP Exchange participation renewal.	S	

Small Business Requirements Traceability Matrix

SH-217	Small Business	Update Employee Application / Renew Employee QHP Participation	OneGate	OneGate	Produce written notification / request for employee to verify key eligibility factors for the purposes of annual eligibility / enrollment renewal and report changes if necessary.	W	
SH-218	Small Business	Update Employee Application / Renew Employee QHP Participation	Oracle Identity Manager	Oracle Identity Manager	Provide capability for employees to look up or reset login credentials.	S	

mall Business Requirements Traceability Matrix

H-219	Small Business	Renew Employee QHP Participation	OneGate	OneGate	Produce a notice of annual open enrollment.	W	
H-220	Small Business	Renew Employee QHP Participation	OneGate	OneGate	Produce notification to employees regarding the number of days left for open enrollment.	W	

Small Business Requirements Traceability Matrix

SH-221	Small Business	Update Employee Application	OneGate	OneGate	Provide capability for employees to submit changes to key eligibility factors for the purpose of annual eligibility / enrollment renewal. Supported methods of reporting changes include written forms and web-based responses through the Exchange.	S	
SH-222	Small Business	Update Employee Application	OneGate	OneGate	Process employee response to renew eligibility and initiate eligibility determination process if necessary. Review employee Exchange eligibility. Have the capability to adjudicate mandatory / optionally reported changes and the resultant changes to	S	

all Business Requirements Traceability Matrix

-223	Small Business	Renew Employee QHP Participation	OneGate	OneGate	Provide the capability to calculate a year-to-date average for premiums paid for display to the employee at time of renewal.	S	
-224	Small Business	Update Employee Application	OneGate	OneGate	If reported changes do not qualify an employee for a special enrollment, store the eligibility / household changes for use during the next available open enrollment period.	S	

mall Business Requirements Traceability Matrix

SH-225	Small Business	Renew Employee QHP Participation	OneGate	OneGate	If the employee's current plan(s) are no longer available, automatically suggest employee participation for a default health plan(s) for a geographic area.	S	
SH-226	Small Business	Renew Employee QHP Participation	OneGate	OneGate	Based on the availability of QHP(s), determine availability of an employee's current plan for the purposes of enrollment renewal.	S	

nall Business Requirements Traceability Matrix

H-227	Small Business	Update Employee Application	OneGate	OneGate	Provide capability for employees to submit changes to Small Business plan participation (selected plan(s), selected tier (optional), covered dependents, etc.). Supported methods of enrollment changes include written forms and web-based responses	S	
H-228	Small Business	Renew Employee QHP Participation	OneGate	OneGate	Based on an employee's responses to enrollment renewal, assess responses for need to initiate enrollment into a new QHP or additional employees (or employers) into an existing QHP.	S	

mall Business Requirements Traceability Matrix

SH-229	Small Business	Employee Enrollment in QHP	OneGate	OneGate	Process notification to employer of coverage for employees. Also, communicate any next steps required by the employer.	W	
SH-230	Small Business	Determine Employee Eligibility	OneGate	OneGate	Provide the functionality to determine if an update to an employee account is categorized as a Qualifying Event.	S	

nall Business Requirements Traceability Matrix

H-231	Small Business	Update Employee Application	OneGate	OneGate	Provide capability for employees to submit changes to employee plan (add / remove dependents) in between redeterminations / renewals and due to qualifying events.	S	
H-232	Small Business	Change Reporting	Healthation	Not healthation / premium processing outsourcer	Prepare and send monthly report to employer with the insurance bill, indicating changes to their employee enrollment list. Some of these changes will result from the employee's reporting of Qualifying Events.	W	

Small Business Requirements Traceability Matrix

SH-233	Small Business	Change Reporting	OneGate	OneGate	Prepare and send communication to the employee regarding changes to the employee's account due to a Qualifying Event.	W	
SH-234	Small Business	Change Reporting	OneGate	OneGate	Initiate enrollment or disenrollment process for employee or the employee's dependents, depending on the nature of the Qualifying Event.	S	

nall Business Requirements Traceability Matrix

H-235	Small Business	Change Reporting	OneGate	OneGate	Provide the capability for employees to submit changes to the employee contact information.	S	
SH-236	Small Business	Change Reporting	Healthation	Not healthation / premium processing outsourcer	Report employee contact information changes to the Issuer.	W	

Small Business Requirements Traceability Matrix

SH-237	Small Business	Change Reporting	OneGate	OneGate	Prepare and send communication to the employee regarding changes to the Employee contact information.	W	
SH-238	Small Business	Periodic Reporting and Reconciliation	OneGate	OneGate	Allow employers and brokers/assisters to view and track the premium payment.	W	

nall Business Requirements Traceability Matrix

H-239	Small Business	Periodic Reporting and Reconciliation	Healthation	Not healthation / premium processing outsourcer	Reconcile enrollment information and employer participation information with QHPs at least monthly.	W	
H-240	Small Business	Billing/Payment	Healthation	Healthation	The system shall provide small businesses with an aggregated monthly bill for the cost of employees' coverage.	W	

Small Business Requirements Traceability Matrix

SH-241	Small Business	Billing/Payment	Healthation	Not healthation / premium processing outsourcer	Provide the ability to facilitate the collection of premiums and send the premiums to the QHP	W	
SH-242	Small Business	Billing/Payment	Healthation	Not healthation / premium processing outsourcer	Support Issuer payments to Brokers and Agents	W	

mall Business Requirements Traceability Matrix

SH-243	Small Business	Billing/Payment	Healthation	Not healthation / premium processing outsourcer	Provide the ability to allocate Exchange operational fees to Issuers	W	
SH-244	Small Business	Billing/Payment	Healthation	Not healthation / premium processing outsourcer	Provide the ability to handle invoice and payment discrepancies	W	

Small Business Requirements Traceability Matrix

SH-245	Small Business	Billing/Payment	Healthation	Not healthation / premium processing outsourcer	Provide a rules engine that manages actions required in the event of employers making advance payments, late payments or do not make payments	W	
SH-246	Small Business	Billing/Payment	Healthation	Not healthation / premium processing outsourcer	The system shall make payments to QHPs on behalf of SHOP enrollees.	W	

Small Business Requirements Traceability Matrix

SH-247	Small Business	Billing/Payment	Healthation	Not healthation / premium processing outsourcer	Support electronic payment methods that support multiple mechanisms such as credit card, online check and electronic funds transfer	W	How to implement "employee choice"

Financial Management Requirements Traceability Matrix

FM-1	Financial Management	APTCs and CSRs	Healthation	OneGate	Generate daily transactional 834 transaction file in a HIPAA compliant format on all individuals enrollment updates for the Exchange	S	
FM-2	Financial Management	APTCs and CSRs	Healthation	OneGate	Transmit daily transactional 834 transaction file in a HIPAA compliant format of individuals enrolled in QHPs to CMS	S	
FM-3	Financial Management	APTCs and CSRs	Healthation	OneGate	Generate monthly 834 transaction file in a HIPAA compliant format of individuals enrolled in the QHPs for the upcoming month along with the amounts of advance tax credits and cost sharing reductions.	F	
FM-4	Financial Management	APTCs and CSRs	Healthation	OneGate/ Oracle BI	Transmit monthly report of individuals enrolled in QHPs to CMS in a file format as specified by CMS.	F	
FM-5	Financial Management	APTCs and CSRs	Healthation	OneGate/ Oracle BI	Transmit monthly report of individuals enrolled in the QHPs to the appropriate Issuers	S	

ancial Management Requirements Traceability Matrix

M-6	Financial Management	APTCs and CSRs	Healthation	OneGate	Update Exchange financial data with tax credit (APTC) and cost sharing reduction (CSR) payments to Issuers.	F	
M-7	Financial Management	APTCs and CSRs	Healthation	Premum Processor	If CMS agrees to allow the Exchange to pay APTC and CSR amounts directly to issuers, the system must aggregate CSRs, APTCs and premiums and pay the Issuers.	F	
M-8	Financial Management	APTCs and CSRs	Healthation	Premium Processor	Provide the ability to receive APTC and CSR premium payment history reports from Issuers.	F	
M-9	Financial Management	APTCs and CSRs	Healthation	OneGate	Receive electronic Issuer payment reports from CMS.	F	
M-10	Financial Management	APTCs and CSRs	Healthation	Oracle BI	Verify results and discrepancies received from CMS of Individual tax credit and CSR amounts against the Exchange Financial Management Database	F	

inancial Management Requirements Traceability Matrix

FM-11	Financial Management	APTCs and CSRs	Healthation	Oracle BI	Provide tools to identify, analyze and resolve APTC and CSR discrpancies between CMS and the Exchange Financial Management database	F	
FM-12	Financial Management	APTCs and CSRs	Healthation	Premium Processor	Update Exchange Financial Management database with electronic issuer payment data.	F	
FM-13	Financial Management	APTCs and CSRs	Healthation	Oracle BI	Compare payments data made by CMS to payment report data provided to CMS and report exceptions.	F	
FM-14	Financial Management	APTCs and CSRs	Healthation	Oracle BI	Provide tool to reconcile and adjust and identified discrpencies between the Exchange Financial Management database and data received from Issuers, and/or CMS.	F	Report only - tool not appropriate for SOV's chosen business process
FM-15	Financial Management	APTCs and CSRs	Healthation	Premium Processor	Receive electronic payment history report from Issuers.	F	

nancial Management Requirements Traceability Matrix

FM-16	Financial Management	APTCs and CSRs	Healthation	Premium Processor	Update Exchange database with Issuer payment history data.	F	
FM-17	Financial Management	APTCs and CSRs	Healthation	Premium Processor	Produce electronic Issuer payment history report and transmit to CMS in a format as determined by CMS.	F	
FM-18	Financial Management	APTCs and CSRs	Healthation	OneGate	Update Individual Eligibility and Enrollment database to reflect discrepancy resolution	F	
FM-19	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Calculated employer premium based on Exchange SHOP enrollment requirements.	S	
FM-20	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Allow for retroactive employee enrollments and retroactive employee determinations and roll these amounts into the next billing cycle for the employer.	S	

Financial Management Requirements Traceability Matrix

FM-21	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Calculate employer fee if applicable.	S	
FM-22	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Update Exchange database with employer fee information.	S	
FM-23	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Support the creation of billing units within employer groups to segregate premium fees	S	
FM-24	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Produce Employer Invoice Notification and email or on paper to Employer.	S	
FM-25	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Produce Employer invoice and e-mail or on paper. The invoice should include the monthly balance due and any outstanding premium payments due as well as employer identifying information	S	

nancial Management Requirements Traceability Matrix

M-26	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Provide capability to "rebill" an existing invoice to a SHOP employer	S	
M-27	Financial Management	SHOP Premium Collection	OneGate	Premium Processor	Provide functionality that allows Employer to create a notification that invoice discrepancy exists.	S	
M-28	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Provide functionailty for Employers to make electronic payments that include e-check, electronic funds transfer, and credit card in compliance with the Payment Card Industry Data Security Standards.	S	
M-29	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Receive and process premium payments.	S	
M-30	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Provide capability to track and enforce premium payment timing guidelines and restrictions	S	

Financial Management Requirements Traceability Matrix

FM-31	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Provide tools for employers to make recurring or scheduled premium payments to the Exchange.	S	
FM-32	Financial Management	SHOP Premium Collection	Healthation	Premium Processor	Provide tools to record, resolve, and track receipt of premium payments in the Exchange database.	S	
FM-33	Financial Management	SHOP Premium Collection	OneGate	Premium Processor	Provide tools for SHOP users to download premium payment history and data	S	
FM-34	Financial Management	SHOP Premium Collection	Healthation	Oracle BI	Identify and account for discrepancies between employer payments and CMS reported payments (reconciliation).	F	
FM-35	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Record individual premium payment option.	S	

nancial Management Requirements Traceability Matrix

M-36	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Calculate individual premium payment amount itemized by billing cycle and by product.	S	
M-37	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	If Basic Health is implemented, calculate the Basic Health premium.	S	
M-38	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Calculate Individual Fee if applicable.	S	
M-39	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Send Invoice notification to individual for monthly premium payment.	S	
M-40	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	The invoice notification would include a link to login to the Exchange and make an electronic payment.	S	

Financial Management Requirements Traceability Matrix

FM-41	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	The invoice should include upcoming month's premium due, year to date paid amounts, and if applicable, prior unpaid premium amounts and adjusted amounts.	S	
FM-42	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Produce electronic or hard-copy monthly premium invoice to individual, itemized by product/program and summarized to one total amount	S	
FM-43	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Provide capability to "rebill" an existing invoice to an individual	S	
FM-44	Financial Management	State Option to Collect Individual Premiums through the Exchange	OneGate	Premium Processor	Provide a view invoice screen for Individual.	S	
FM-45	Financial Management	State Option to Collect Individual Premiums through the Exchange	OneGate	Premium Processor	Provide invoice discrepancy notification capabilities for Individual to Exchange.	S	

nancial Management Requirements Traceability Matrix

M-46	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Provide the ability for individuals to pay premium via electronic payment on Exchange with options to pay by e-check, electronic funds transfer and credit card in compliance with the Payment Card Industry Data Security Standards.	S	
M-47	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Support E-check and ACH processing for payment remittance	S	
M-48	Financial Management	State Option to Collect Individual Premiums through the Exchange	OneGate	Premium Processor	Provide tools for individuals to make recurring or scheduled premium payments to the Exchange.	S	
M-49	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Receive and process premium payments from individuals.	S	
M-50	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Provide capability to track and enforce premium payment timing guidelines and restrictions	S	

inancial Management Requirements Traceability Matrix

FM-51	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Update database with financial information about electronic payments and payment type.	S	
FM-52	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Track premium payments by individuals, including information related to payment type	S	
FM-53	Financial Management	State Option to Collect Individual Premiums through the Exchange	OneGate	Premium Processor	Provide tools for individual users to download premium payment history and data	S	
FM-54	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Produce payment exception report and notification to individual.	S	
FM-55	Financial Management	State Option to Collect Individual Premiums through the Exchange	Healthation	Premium Processor	Produce report on comissions due to brokers as a result of enrollment transactions	S	

ancial Management Requirements Traceability Matrix

M-56	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Periodically and on demand identify and produce reports on unpaid employer premiums for SHOP enrollees, including unpaid amounts or incorrect payment amounts.	S	
M-57	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Produce notifications to employers regarding unpaid/incorrectly paid premium amounts	S	
M-58	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Send notification of unpaid premiums to employers.	S	
M-59	Financial Management	Employer Premium Discrepancy Resolution	OneGate	Premium Processor	Receive Employer invoice discrepancy notification.	S	
M-60	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Provide inquiry screens to identify the source of the discrepancy and make note of it electronically.	S	

inancial Management Requirements Traceability Matrix

FM-61	Financial Management	Employer Premium Discrepancy Resolution	Siebel Public Sector CRM	Premium Processor	Produce Notification to authorized users of the reported discrepancy.	W	
FM-62	Financial Management	Employer Premium Discrepancy Resolution	OneGate	Premium Processor	Provide capability for employers to updated employer account and make adjustments.	S	
FM-63	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Interface with Exchange general ledger system to update corresponding subsidiary ledger accounts.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
FM-64	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Generate invoice adjustment (positive or negative).	S	
FM-65	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Allow for tolerance acmount on receipt of payment. System should be able to support either dollar amount or percentage tolerace levels.	S	

nancial Management Requirements Traceability Matrix

FM-66	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Identify payments that are outside of the accepted tolerance amount.	S	
FM-67	Financial Management	Employer Premium Discrepancy Resolution	Healthation	Premium Processor	Provide for processing adjustments for bad checks or payments due to NSF or other reasons. Functionaly may included reversing or adding fees for failed transctions.	S	
FM-68	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Provide automated process for identifying unpaid individual premiums and/or premium payment discrepancies	S	
FM-69	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Provide automated processing to generate a notification to the individuals regarding unpaid premiums and/or premium discrepancies.	S	
FM-70	Financial Management	Individual Premium Discrepancy Resolution	OneGate	Premium Processor	Provide ability to read Individual notifications online regarding invoice discrepancies.	W	

Financial Management Requirements Traceability Matrix

FM-71	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Send notifications of unpaid premiums to Individuals.	S	
FM-72	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Provide automated process to identify invoice discrepancies from an individual.	S	
FM-73	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Provide notification to individual that discrepancy report was received from the individual.	S	
FM-74	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Provide inquiry screens to identify the source of the discrepancy and make notes about what needs to be corrected.	S	
FM-75	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Produce notification to the Eligibility and Enrollment database of the discrepancy.	F	

inancial Management Requirements Traceability Matrix

FM-76	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Provide automated process to update the individual account with an invoice adjustment as a result of a discrepency resolution.	S	
FM-77	Financial Management	Individual Premium Discrepancy Resolution	Healthation	NA	Update corresponding subsidiary ledger accounts.	S	NA under SOVs expected business process
FM-78	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Generate and send invoice adjustment (positive or negative).	S	
FM-79	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Allow for tolerance acmount on receipt of payment. System should be able to support either dollar amount or percentage tolerace levels.	S	
FM-80	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Identify payments that are outside of the accepted tolerance amount.	S	

Financial Management Requirements Traceability Matrix

FM-81	Financial Management	Individual Premium Discrepancy Resolution	Healthation	Premium Processor	Provide for processing adjustments for bad checks or payments due to NSF or other reasons. Functionaly may included reversing or adding fees for failed transctions.	S	
FM-82	Financial Management	Issuer Payment Reconciliation	Siebel Public Sector CRM	Premium Processor	Receive electronic or telephonic notification of discrepancy from Issuer.	S	
FM-83	Financial Management	Issuer Payment Reconciliation	Healthation	Premium Processor	Provide authorized Exchange users a method to review and modify the Exchange financial records for payment descrepencies identified by the Issuer.	S	
FM-84	Financial Management	Issuer Payment Reconciliation	Healthation	Premium Processor	Provide appropriate access and functionality to Customer Service workers to Exchange records regarding invoice discrepancies to support CS resolution activities	W	
FM-85	Financial Management	Issuer Payment Reconciliation	Healthation	Premium Processor	The system will provide screens to update Exchange records with corrected invoice / payment information for Issuers, Employers, or Individual records.	S	

nancial Management Requirements Traceability Matrix

M-86	Financial Management	Risk Adjustment Calculation	Healthation	Oracle BI	Provide regular reports and data on Exchange enrollees to support risk adjustment calculations. Data will include, but is not limited to: unique individual identifier, plan enrolled in, the type of coverage purchased, rating criteria information, demographic data, and	S	
M-87	Financial Management	Risk Adjustment Calculation	Healthation	Oracle BI	Provide regular reports and data on QHPs and encounters to CMS to support risk adjustment calculation.	S	
M-88	Financial Management	Risk Adjustment Calculation	Healthation	N/A	Provide the capacity to electronically receive information from Issuers on non-exchange enrollees from individual, small group, and self-funded plans inside and outside of the state	F	
FM-89	Financial Management	Risk Adjustment Calculation	Healthation	OneGate	Provide the capacity to electronically receive non QHP plan and rate setting data from CMS and other state sources	F	
FM-90	Financial Management	Risk Corridors	Healthation	Oracle BI	Extract and send Individual and SHOP Plan data to CMS for risk corridors	F	

Financial Management Requirements Traceability Matrix

FM-91	Financial Management	Risk Corridors	Healthation	OneGate	Receive unpaid Risk Corridor Charge information from CMS	F	
FM-92	Financial Management	Plan Assessment (fees) for State Exchange Operations	Healthation	Premium Processor	The system will calculate the user fee from Issuers and update the financial accounts. Charging Issuers should be a configurable option.	S	
FM-93	Financial Management	Plan Assessment (fees) for State Exchange Operations	Healthation	Premium Processor	Support multiple categories or levels of fees.	S	
FM-94	Financial Management	Plan Assessment (fees) for State Exchange Operations	Healthation	Premium Processor	The Issuer invoice will be generated and a Notification sent to the Issuer.	S	
FM-95	Financial Management	Plan Assessment (fees) for State Exchange Operations	Healthation	Premium Processor	Provide functionailty for Issuers to make electronic payments of user fees include e-check, electronic funds transfer, and credit card in compliance with the Payment Card Industry Data Security Standards.	S	

Financial Management Requirements Traceability Matrix

FM-96	Financial Management	Plan Assessment (fees) for State Exchange Operations	Healthation	Premium Processor	The system will allow for the fee to reduce the amount of premiums the Exchange pays the Issuer as an alternative.	F	
FM-97	Financial Management	Plan Assessment (fees) for State Exchange Operations	Healthation	Premium Processor	Provide data extract of receipt of user fees to support Annual Financial Reporting for the Exchange	F	
FM-98	Financial Management	Issuer Payment Transfers	Healthation	Premium Processor	The system will aggregate premium payments for each Issuer.	F	
FM-99	Financial Management	Issuer Payment Transfers	Healthation	Premium Processor	The system will perform the aggregation on a monthly basis.	F	
FM-100	Financial Management	Issuer Payment Transfers	Healthation	Premium Processor	The system will account for the type of fee being charged and aggregate the correct amount for the Issuer.	F	

Financial Management Requirements Traceability Matrix

FM-101	Financial Management	Issuer Payment Transfers	Healthation	Premium Processor	Alternative, CMS would pay APTC and CSR amounts to the Exchange and the Exchange would aggregate them and pay Issuers.	F	
FM-102	Financial Management	Issuer Payment Transfers	Healthation	Premium Processor	If the Basic Health option is implemented, then any APTC that individuals may qualify for will be remitted to the State.	F	
FM-103	Financial Management	Issuer Payment Transfers	Healthation	Premium Processor	Provide electronic notification to Issuers upon transfer of payments to the Issuers	F	
FM-104	Financial Management	Reinsurance Contribution Verification	Healthation	Premium Processor	Extract and summarize Exchange enrollee and premium data and provide the data to the Reinsurance entity to verify reinsurance contribution from Issuer	S	
FM-105	Financial Management	Exchange Internal Accounting	Healthation	Premium Processor	Track and report on user fees received by the Exchange to support Exchange operations	F	

Financial Management Requirements Traceability Matrix

FM-106	Financial Management	Exchange Internal Accounting	Business Objects	NA	Track operational and overhead expenses of the Exchange.	C	NA under SOVs expected business process
FM-107	Financial Management	Exchange Internal Accounting	Healthation	NA	The system will summarize and apply general ledger coding to the financial transactions.	W	NA under SOVs expected business process
FM-108	Financial Management	Exchange Internal Accounting	Healthation	NA	The system will update the Exchange Financial Management database.	S	NA under SOVs expected business process
FM-109	Financial Management	Exchange Internal Accounting	Healthation	NA	Transmit the general ledger transactions to the accounting system.	W	NA under SOVs expected business process
FM-110	Financial Management	Exchange Internal Accounting	Healthation	Oracle BI	The Exchange will provide detail reports to support and reconcile the Exchange Annual Financial Report.	W	

Financial Management Requirements Traceability Matrix

FM-111	Financial Management	Exchange Internal Accounting	Healthation	NA	Provide adequate internal controls for monitoring and preventing fraud, waste and abuse	W	NA under SOVs expected business process
FM-112	Financial Management	Exchange Internal Accounting	Business Objects	Oracle BI	Create regular and ad-hoc reporting on an as-needed basis to govern and monitor the Exchange financial health	M	
FM-113	Financial Management	Exchange Internal Accounting	Business Objects	Oracle BI	Create the Exchange Annual Financial Report data as required by CMS and other state entities	M	
FM-114	Financial Management	Cash Management	Healthation	Premium Processor	Support the management of cash receipts for premium payments, including the provisioning of a lockbox, and the tracking the accounting and reconciliation of cash receipts	S	

Administrative Requirements Traceability Matrix

A-1	Audit	Data Quality	Oracle Enterprise Data Quality	Oracle Enterprise Data Quality	Perform periodic analysis of data for accuracy and potential individual contact for verification, and potentially, follow-up on incomplete information (e.g., dummy DOB or SSN)	**S**	
A-2'	Audit	Eligibility Determination	OneGate	OneGate	Maintain data to produce a report of the outcomes of rules exectution for all eligibility determinations (positive or negative) for appeals research and to analyze correctness of eligibility functionality.	S	

A-3	Audit	Transfer of Identification Information	All, as appropriate	All, as appropriate	The Exchange must maintain an audit trail of all information requests that contain Personal Identification (PII) or Personal Health Information (PHI) data as specified by the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA).	S	
A-4	Audit	IRS Tax Information	All, as appropriate	All, as appropriate	The Exchange shall comply with any security and privacy requirements established by the IRS (e.g., Publication 1075 Tax Information Security Guidelines for Federal, State, and Local Agencies) to ensure proper and confidential handling and storage of Section 6103 Federal Tax Information data. In addition, any system handling tax information shall have audit trails that meet IRS standards.	S	
A-5	Audit	Risk Adjustment, Risk Corridors, and Reinsurance	Business Objects	Oracle BI	The Exchange must make certain claims and encounter data collected for the purposes of risk adjustment calculation are available to support other activities including, but not limited to: recalibrating Federally-certified risk adjustment models; verifying of risk corridor submissions; and verifying and auditing reinsurance claims.	M	The CGI team will develop the Vermont specific reports through Oracle BI for HBE operations.

A-6	Audit	Security	All, as appropriate	All, as appropriate	To adequately respond to "breach notification requirements," the Exchange should maintain an audit trail to aid in recreating a security incident and determining the extent of the security breach. This data will aid in identifying who must be notified rather than having to notify all individuals.	S	
A-8	Program Integrity	Identity Management	Oracle Enterprise Data Quality	Oracle Enterprise Data Quality	Retain sufficent data to allow periodic sampling and analysis to identify potential fraud, waste, and abuse.	S	
	Program Integrity	Individual Identification	Oracle MDM (Customer Hub)	Oracle MDM (Customer Hub)	Retain sufficient data to allow periodic analysis of potentially duplicate individuals	S	

	Program Integrity	Individual Identification	Oracle MDM (Customer Hub)	Oracle MDM (Customer Hub)	Provide the ability to successfully merge/unmerge potential duplicate individual records	S	
A-9	Program Integrity	Individual Identification	OneGate	OneGate	The Exchange needs to keep track of all individual identity changes (e.g., marriage, legal name change, etc.) so that name searches under any name an individual has been know will be successful.	S	
A-11	Program Integrity	Retroactive Eligibility Reconciliation	OneGate	OneGate	Provide the ability to process retroactive eligibility changes including the reconciliation of insurance coverage payments.	S	

	Web Analytics	Web Analytics	Google Analytics	Google Analytics	Provide web analytics tools comparable to Google Analytics	S	
	Web Analytics	Web Analytics	Splunk	Splunk	Provide the capability to review raw web logs for usability and security analyses	S	
A-19	Business Analytics	SHOP, EE,Plan Management	Business Objects	Oracle BI	The specific BI requirements for Exchange data have not been identified, but it will involve KPI definition, trend analysis, forecasting, statistical analysis, and aggregation of eligibility, enrollment and plan data. This data will include, but is not limited to: - Cost breakdown per individual - Cost breakdown per employee (SHOP) - Cost breakdown per employer - Plan data	M	The CGI team will develop the Vermont specific reports through Oracle BI for HBE operations.

A-20	Business Analytics	Platform	Business Objects	Oracle BI	The business analytics solution for the Exchange should not impact transactional database performance.	S	
A-21	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to generate ad hoc reports.	S	
A-22	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to download and save report data to individual workstations and applications.	S	

A-23	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to transmit reports to various designated recipients in a secure manner.	S	
A-24	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to roll-up (summarize data) and drill-down (view details) in reports online.	S	
A-25	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to schedule the generation of reports at specific times.	S	

A-26	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to notify and distribute reports based on user specified criteria.	S	
A-27	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to organize reports into a shared list (library).	S	
A-28	Business Analytics	Platform	Business Objects	Oracle BI	The system must restrict access to the shared list (library) or items within a shared list (library) to designated users.	S	

A-30	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to sort data within reports in multiple ways.	S	
A-31	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to present data in graphical or chart format.	S	
A-32	Business Analytics	Platform	Business Objects	Oracle BI	The system must provide the ability to limit report views based on user security / access rights.	S	

A-33	Business Analytics	Platform	Business Objects	Oracle BI	The system must allow the user to export formatted reports from the system in industry standard formats.	S	
A-34	Data Processing	Data Upload	Informatica	Informatica	Allow uploads from authorized sources of data necessary to operate the Exchange	W	

Summarized Reporting Requirements Traceability Matrix

RP-1	Reporting	Business Analytics	Business Objects	Oracle BI	Provide a business analytics solution for the Exchange that will use a data warehouse for business intelligence, predictive analytics, and reporting.	S	
RP-2	Reporting	Business Analytics	Business Objects	Oracle BI	Enable ad hoc query and reporting capability by authorized users	S	
RP-3	Reporting	Business Analytics	Business Objects	Oracle BI	Store and recall saved queries created by authorized users	S	
RP-4	Reporting	Business Analytics	Business Objects	Oracle BI	Track and maintain history of all ad hoc queries and reports run within the system	S	

Summarized Reporting Requirements Traceability Matrix

RP-5	Reporting	Business Analytics	Business Objects	Oracle BI	The data warehouse must, at a minimum, include the following dimensions: - Demographic dimension - Geographic dimension (including the entire State of VT)	M	The CGI team will develop the VT specific reports through Oracle B
RP-6	Reporting	Eligibility and Enrollment	Healthation	Premium Provider / OneGate / other approach	Generate a report to a qualified health plan issuer regarding the Exchange's records of current enrollment with the qualified health plan issuer. This report is used to reconcile enrollment records between the Exchange and the qualified health plan issuer.	M	The CGI team will develop the VT specific reports through Oracle B
RP-7	Reporting	Financial Management	Healthation	Premium Provider / OneGate / other approach	Provide financial management reporting including: - Cost and administrative per plan - Issuers - Plans - Benefit structure - Plan rates	S	
RP-8	Reporting	Financial Management	Business Objects	Oracle BI	Provide Exchange Enrollee Data to Risk Adjustment Entity	M	

Summarized Reporting Requirements Traceability Matrix

RP-9	Reporting	Financial Management	Business Objects	Oracle BI	Generate Monthly Report on Individual Enrollment in Qualified Health Plan	M	
RP-10	Reporting	Financial Management	Business Objects	Oracle BI	Generate report of Individual Premium Payment History to CMS	M	
RP-11	Reporting	Financial Management	Business Objects	Oracle BI	Generate and Send Enrollment Discrepancy Reports to Issuer and CMS	M	
RP-12	Reporting	Financial Management	Business Objects	Oracle BI	The Exchange will provide detail reports to support and reconcile the Annual Financial Report.	M	

Summarized Reporting Requirements Traceability Matrix

RP-13	Reporting	Plan Management	Business Objects	Oracle BI	Provide regular reporting on Plan Data to CMS. Schéma should include: - Enrollment - Cost and administrative per plan - Issuers - Plans - Benefit structure - Plan rates - Complaints	M	
RP-14	Reporting	Plan Management	Business Objects	Oracle BI	Report on tranparancy and quality data to CMS	M	
RP-15	Reporting	Plan Management	Business Objects	Oracle BI	Send notification of Change in Enrollment Availability to CMS	M	

Summarized Reporting Requirements Traceability Matrix

RP-16	Reporting	Plan Management	Business Objects	Oracle BI	Provide the ability the plan information on the public exchange view, including data such as: - Plan title and description - Plan quality rating - Plan providers - Out of pocket limits - Annual deductable - Doctor Choice - Prescription Choice - Monthly Premium - Applicants Denied - Plan Details - to be determined - Link to Issuer/Plan website - Medical loss ratio - Transparency in coverage - Summary in benefits and coverage - Levels of coverage - Availability of in-network and out-of-network providers	M	
RP-17	Reporting	Plan Management	Business Objects	Oracle BI	Provide periodic report to the Federeal Data Services Hub to submit required data to CMS, but not limited to: - Issuer data - Plan data including - Benefits structure - rates - enrollment	M	

Summarized Reporting Requirements Traceability Matrix

RP-18	Reporting	Plan Management	CGI Plan Management	CGI Plan Management	The system must provide a compliance dashboard to indicate compliance analysis progress on Issuers/plans and the results of the compliance analysis through the compliance process	M	
RP-19	Reporting	Plan Management	Business Objects	Oracle BI	The system must provide a Issuer performance indicator dashboard to aggregate performance data and display summary performance information by Issuer/Plan	M	
RP-20	Reporting	Plan Management	CGI Plan Management	CGI Plan Management	Provide interface/query to Federal Data Services Hub to return data about an Issuer - data could include: - Premium review results - Complaints - Rates of app denial - Claims processing timeliness - Claims denials - Quality reporting	C	CGI will develop the necessary interfaces, using the ESB, with Federal and State Agencies as necessary to comply with ACA requirements.
RP-21	Reporting	Plan Management	CGI Plan Management	CGI Plan Management	Reporting on historical plan acceptance criteria	M	

Summarized Reporting Requirements Traceability Matrix

RP-22	Reporting	Plan Management	CGI Plan Management	CGI Plan Management	Retain and report on periodic historical plan quality ratings as determined by the Exchange.	W	
RP-23	Reporting	Plan Management	CGI Plan Management	CGI Plan Management	The system must be able to display a variety of data about a plan to help determine the decision to renew including: - Issuer Performance Data - Quality Data - Complaint Data - Coverage data - Benefits and rates	W	
RP-24	Reporting	Plan Management	Siebel Public Sector CRM	Siebel Public Sector CRM	The system must be able to track and manage complaints and consumer feedback about Issuers filed through the Exchange.	W	
RP-25	Reporting	Plan Management	Siebel Public Sector CRM	Siebel Public Sector CRM	The system must report on Exchange user complaint data on a periodic basis. Complaint data can include: - Issuer - Number of complaints - Complaint type - Complaint description/detail	W	

Summarized Reporting Requirements Traceability Matrix

Summarized Noticing Requirements Traceability Matrix

NO-1	Notification	UX	OneGate	OneGate	Users of the Exchange Web portal can view the history of all communication between the Exchange and the individual online	W	
NO-2	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Provide the capability to target noticing at a family/household or individual level	S	
NO-3	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Support the message body in a variety of fomats including, but not limted to text, RTF, or HTML	S	
NO-4	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Provide the capability to pass parameters to both the title and the body of the notification	S	
NO-5	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Include graphics capability for notifications	S	
NO-6	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Enforce size requirements on messages as defined by the Exchange	S	
NO-7	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Recognize "opt-out" flags attached to individual records and supress notifications to those indivdiuals	W	
NO-8	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Recognize and "invalid e-mail" flag and supress notifications to those addresses	W	
NO-9	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Filter out and supress live e-mails for notification test instances	W	
NO-10	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Assign a notification ID (notification event) and include on all messages as determined by the Exchange	W	
NO-11	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Support barcoding of outgoing notifications	W	
NO-12	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Provide the capability to include both dynamic and static attachments	S	
NO-13	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Allow for embeded links within notification message	S	
NO-14	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Provide tools to manage e-mail "bouncebacks", including the ability to parse the "bounceback" message for actions	W	
NO-15	Notification	Notification Engine	Thunderhead NOW	Thunderhead NOW	Provide the capability to include the message ID in the notification subject line	S	
NO-16	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	Notify Employer of Payment Discrepancy	W	

Summarized Noticing Requirements Traceability Matrix

NO-17	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	Provide Invoices to Individuals	W	
NO-18	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	Provide notifications to employers of payment discrepancy from Small Business	W	
NO-19	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	Provide notification to individuals of payment discrepancy from Exchange	W	
NO-20	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	The Issuer invoice will be generated and a Notification sent to the Issuer.	W	
NO-21	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	Produce Notification to Eligibility and Enrollment of the discrepancy.	W	
NO-22	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	Send notification of unpaid premiums to employers.	W	
NO-23	Notification	Financial Management	Healthation	Premium Processor / OneGate / other options	The invoice notification would include a link to login to the Exchange and make an electronic payment.	W	
NO-24	Notification	Eligibility and Enrollment	OneGate	OneGate	Produce a mailed, written notice to the individual to provide additional verifications; the automated written notice shall include: - Individual name, - Address - Unique identifier - Information requested - Due date based on date of initial application	W	
NO-25	Notification	Eligibility and Enrollment	OneGate	OneGate	Send notification for change in individual's Eligibility Status	W	

Summarized Noticing Requirements Traceability Matrix

NO-26	Notification	Eligibility and Enrollment	OneGate	OneGate	When additional verification is required, provide on-screen notification to individual to supply additional verifications through the exchange.	W	
NO-27	Notification	Eligibility and Enrollment	OneGate	OneGate	Generate on-screen notification to individuals who select at Tax Credit Advance of the possibility of tax penalties / liabilities at time of tax filing should their annual income increase.	W	
NO-28	Notification	Eligibility and Enrollment	Healthation	Premium Processor / OneGate / other options	Prepare an electronic, real-time transmission of information necessary in order for the qualified health plan issuer to provide a welcome package and identification card to the individual and to implement advance premium tax credits and cost-sharing reductions, as applicable.	W	
NO-29	Notification	Eligibility and Enrollment	OneGate	OneGate	Generate communication to individual requesting additional documentation to support his/her attestation of annual / monthly income. This should only occur when the Exchange is not able to verify income via authoritative sources.	W	
NO-30	Notification	Eligibility and Enrollment	OneGate	OneGate	Prepare and provide communication to individuals about a mid-year plan decertification and notify need for plan selection / enrollment.	W	
NO-31	Notification	Eligibility and Enrollment	OneGate	OneGate	Prepare written and on-screen notification to individuals regarding eligibility for enrollment periods.	W	
NO-32	Notification	Eligibility and Enrollment	Healthation	Premium Processor / OneGate / other options	Prepare an electronic notice to CMS with a minimum dataset of information regarding an individual's enrollment in a qualified health plan through the Exchange. This information is used to generate payments to qualified health plan issuers for advance premium tax credits and cost-sharing reductions, as well as for performance measurement and tax administration, as applicable.	F	

Summarized Noticing Requirements Traceability Matrix

NO-33	Notification	Eligibility and Enrollment	Healthation	Premium Processor / OneGate / other options	Provide notification to the issuer of an individual's selected qualified health plan regarding changes to the individual's information, including to his or her levels of advance premium tax credits or cost-sharing reductions, or regarding a decision by an individual to renew his or her enrollment in the qualified health plan.	F	Will work with VT to identify appropriate method to address.
NO-34	Notification	Eligibility and Enrollment	Business Objects	Oracle BI	Notify CMS regarding reconciled periodic enrollment information. This information is used to generate payments to qualified health plan issuers for advance premium tax credits and cost-sharing reductions, as well as for performance measurement and tax administration, as applicable.	M	The CGI team will develop the VT specific reports for operations.
NO-35	Notification	Eligibility and Enrollment	OneGate	OneGate	If an individual initiates a voluntary disenrollment through the Exchange and not directly with the Issuer, produce an electronic notification to the Issuer to disenroll an individual.	W	
NO-36	Notification	Eligibility and Enrollment	Healthation	Premium Processor / OneGate / other options	Prepare a notice to CMS with a minimum dataset of information regarding an individual's disenrollment from a qualified health plan through the Exchange. This information is used to adjust payments to qualified health plan issuers for advance premium tax credits and cost-sharing reductions, as well as for performance measurement and tax administration, as applicable.	W	
NO-37	Notification	Eligibility and Enrollment	OneGate	OneGate	Generate written and on-screen notification of the result of an individual's eligibility determination (including information such as individuals evaluated, MAGI used for basis of determination, period of eligibility, etc.) Notifications must align with currently established eligibility notices for Medicaid and CHIP.	W	
NO-38	Notification	Eligibility and Enrollment	OneGate	OneGate	Provide electronic notification to CMS of the result of an individual's eligibility determination.	W	

Summarized Noticing Requirements Traceability Matrix

NO-39	Notification	Eligibility and Enrollment	Siebel Public Sector CRM	Siebel Public Sector CRM	Generate a notification to CMS of any completed appeals decisions.	W	
NO-40	Notification	Eligibility and Enrollment	OneGate	OneGate	Send a formal, written notice to a individual's mailing address summarizing eligibility determination for individual exemption	W	
NO-41	Notification	Eligibility and Enrollment	OneGate	OneGate	Send an automated transaction individuals who have been determined as exempt or not exempt to CMS	W	
NO-42	Notification	Eligibility and Enrollment	OneGate	OneGate	Send a formal, written notice to a individual's mailing address summarizing eligibility determination for individual exemption	W	
NO-43	Notification	Small Business	OneGate	OneGate	Upon submittal of initial Employer Application, provide email and written notification to employees (as identified on the employee roster) to elect for or opt-out of employer sponsored coverage. Notification should also provide instructions and information to the employee about the open enrollment period and SHOP website access.	S	
NO-44	Notification	Small Business	OneGate	OneGate	Provide ability to generate on-screen and written notification to employers who select at Small Business Tax Credit of the possibility of tax penalties / liabilities at time of tax filing should their business size or income change.	S	
NO-45	Notification	Small Business	OneGate	OneGate	Produce a mailed, written notice to the employer to provide additional verifications; the automated written notice shall include: - Employer name - Address - Unique identifier, potentially - Employer EIN - Information requested - Due date based on date of initial application	S	

Summarized Noticing Requirements Traceability Matrix

NO-46	Notification	Small Business	OneGate	OneGate	If an employer has an involuntary termination through the Exchange, produce an electronic notification to the Issuer to terminate the employer. Also produce an electronic notification to the employer's employees to inform them of the employer termination.	S	
NO-47	Notification	Small Business	OneGate	OneGate	Prepare a notice to CMS with a minimum dataset of information regarding an employer's involuntary termination from a qualified health plan through the Exchange. This information may be used for small business tax credits, as well as for individual mandates, etc., as applicable.	S	
NO-48	Notification	Small Business	OneGate	OneGate	Produce written notification / request for employers to verify key eligibility factors (continue to has a current EIN, etc.) for the purposes of annual eligibility / participation renewal and report changes if necessary.	S	
NO-49	Notification	Small Business	OneGate	OneGate	Produce a notice of annual open enrollment.	S	
NO-50	Notification	Small Business	OneGate	OneGate	In all notices produced by the Exchange regarding eligibility determination, notify employers to their rights and responsibilities (including a right to appeal eligibility decisions).	S	
NO-51	Notification	Small Business	Siebel Public Sector CRM	Siebel Public Sector CRM	Generate a formal written notice informing an employer of the details of an appeal decision.	S	
NO-52	Notification	Small Business	Siebel Public Sector CRM	Siebel Public Sector CRM	Generate a notification to CMS of any completed appeals decisions.	S	
NO-53	Notification	Small Business	OneGate	OneGate	Generate a notification to an employer regarding the employer's adjusted eligibility determination based on the employer's Exchange eligibility appeal decision.	S	

Summarized Noticing Requirements Traceability Matrix

NO-54	Notification	Small Business	OneGate	OneGate	Produce a mailed, written notice to the employee to provide additional verifications; the automated written notice shall have the capability to include: - Employee name - Employee Address - Social security number - Other Employee Contact Information - Employer Name - Worksite Address - Enrollees' dependent Information - Information requested - Due date based on date of initial application - Unique identifier, if required	S	
NO-55	Notification	Small Business	OneGate	OneGate	Generate written and on-screen notification of the result of an employee's eligibility determination	S	
NO-56	Notification	Small Business	OneGate	OneGate	Produce an automated and real-time, electronic notification of plan selection.	S	
NO-57	Notification	Small Business	OneGate	OneGate	If an employee initiates a voluntary disenrollment through the Exchange, produce an electronic notification to the employee's employer to inform them of the employee disenrollment.	S	
NO-58	Notification	Small Business	OneGate	OneGate	If an employee initiates a voluntary disenrollment through the Exchange, produce an electronic notification to the Issuer to disenroll the employee.	S	
NO-59	Notification	Small Business	OneGate	OneGate	Prepare a notice to CMS with a minimum dataset of information regarding an employee's disenrollment from a qualified health plan through the Exchange. This information is used for tax administration, as applicable.	S	
NO-60	Notification	Small Business	OneGate	OneGate	If an employee has an involuntary disenrollment through the Exchange, produce an electronic notification to the employee to inform the employee of the employee disenrollment.	S	

Summarized Noticing Requirements Traceability Matrix

NO-61	Notification	Small Business	OneGate	OneGate	If an employee has a disenrollment through the Exchange, produce an electronic notification to the employee's employer to inform them of the employee termination and alternative insurance options.	S	
NO-62	Notification	Small Business	OneGate	OneGate	Produce written notification / request for employee to verify key eligibility factors for the purposes of annual eligibility / enrollment renewal and report changes if necessary.	S	
NO-63	Notification	Small Business	OneGate	OneGate	Produce a notice of annual open enrollment.	S	
NO-64	Notification	Small Business	OneGate	OneGate	Process notification notifying employer of coverage for employees. Also, communicate any next steps required by the employer.	S	
NO-65	Notification	Small Business	OneGate	OneGate	Provide capability to generate a notification to CMSof any completed appeals decisions.	S	
NO-66	Notification	Small Business	OneGate	OneGate	Generate a notification to an employee regarding the employee's adjusted eligibility determination based on the employee's Exchange eligibility appeal decision.	S	
NO-67	Notification	Small Business	OneGate	OneGate	Prepare and send communication to the employer regarding changes to the Employer's worksite locations.	S	
NO-68	Notification	Small Business	OneGate	OneGate	Prepare and send communication to the employer regarding changes to the employer's employee roster.	S	
NO-69	Notification	Small Business	OneGate	OneGate	Prepare and send communication to the employee regarding changes to the Employee contact information.	S	
NO-70	Notification	Small Business	OneGate	OneGate	Report employee contact information changes to the Issuer.	S	
NO-71	Notification	Small Business	OneGate	OneGate	Prepare and send communication to the employee regarding changes to the employee's account due to a Qualifying Event.	S	

Summarized Noticing Requirements Traceability Matrix

NO-72	Notification	Small Business	OneGate	OneGate	Prepare and send monthly report to employer with the insurance bill, indicating changes to their employee enrollment list. Some of these changes will result from the employee's reporting of Qualifying Events.	S	
NO-73	Notification	Small Business	OneGate	OneGate	Process notification notifying employer of coverage for employees. Also, communicate any next steps required by the employer.	S	
NO-74	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Provide the ability to generate letter of denial indicating that an Issuer and/or Plan has not been accepted into the Exchange	W	
NO-75	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Produce electronic and paper notices for Issuers indicating the results of the compliance and quality reviews, i.e. the compliance and quality rating determination	W	
NO-76	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Produce electronic and paper notices to Issuers when a plan is not renewed to be in the Exchange	W	
NO-77	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon request, generate and send renewal request to Issuers about the plans desired to be renewed, requesting a notification of intent to renew.	W	
NO-78	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon request, generate and send non-renewal notices to Issuers about the plans not be renewed.	W	
NO-79	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon request, generate and send electronic decertification notices to Issuers about the plans to be decertfied.	W	
NO-80	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon request, generate and send letter (mail) decertification notices to Issuers about the plans to be decertfied.	W	

Summarized Noticing Requirements Traceability Matrix

NO-81	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Provide the ability to send electronic notification to the Insurance Division about a non-renewal or decertification of a plan.	W	
NO-82	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Provide the ability to send electronic notification to the appropriate CMS system for plan management and fiscal management functions about a non-renewal or decertification of a plan.	W	
NO-83	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Recertify the plan and notify issuers consistent with the initial certification process.	W	
NO-84	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Update CMS with plan certified plan information consisten with the initial certification processs	W	
NO-85	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon rate approval, send updated plan/rate/benefit data to the appropriate CMS system for plan management and fiscal management functions for determination of silver plans.	W	
NO-86	Notification	Plan Management	CGI Plan Management	CGI Plan Management	If a rate increase is denied, generate a denial notice to the issuer both electronically, and as a formal notice that can be mailed.	W	
NO-87	Notification	Plan Management	CGI Plan Management	CGI Plan Management	If a rate increase is approved, generate an approval notice to the issuer both electronically, and as a formal notice that can be mailed.	W	
NO-88	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Screen submitted rate and benefit data and provide formatting error information back to the Issuer if data format is not correct	W	
NO-89	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Provide the ability to provide submitted rate and benefit data to the Insurance Division system electronically	W	
NO-90	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Registered Navigators/Brokers must be able to subscribe to Exchange notifications	W	
NO-91	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Produce electronic or paper notices for Issuers indicating the results of the compliance and quality reviews, i.e. the compliance and quality rating determination	W	
NO-92	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Produce electronic or paper notices to Issuers when a plan is not renewed to be in the Exchange	W	
NO-93	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Produce electronic or paper notices to Issuers when a plan is not decertified from Exchange	W	

Summarized Noticing Requirements Traceability Matrix

NO-94	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Record the plan or issuer decertification event and status information, including date, reason/rationale.	W	
NO-95	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Produce electronic notification to the Insurance Division when a Issuer/plan is not renewed or is decertified from the Exchange	W	
NO-96	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Produce electronic notification to CMS when an Issuer/plan is not renewed or is decertified from the Exchange	W	
NO-97	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Generate and send renewal request to Issuers about the plans desired to be renewed, requesting a notification of intent to renew.	W	
NO-98	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon request, generate and send non-renewal notices to Issuers about the plans not be renewed.	W	
NO-99	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon request, generate and send electronic decertification notices to Issuers about the plans to be decertfied.	W	
NO-100	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Upon request, generate and send letter (mail) decertification notices to Issuers about the plans to be decertfied.	W	
NO-101	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Provide the ability to send electronic notification to the Insurance Division about a non-renewal or decertification of a plan.	W	
NO-102	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Provide the ability to send electronic notification to the appropriate CMS system for plan management and fiscal management functions about a non-renewal or decertification of a plan.	W	
NO-103	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Generate re-amendment notification and information storage consistent with the initial certification amendment process.	W	

Summarized Noticing Requirements Traceability Matrix

NO-104	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Update CMS with plan certified plan information consisten with the initial certification processs	W	
NO-105	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Provide notices to be sent to plan consumers if a provider network change requires consumer notification.	W	
NO-106	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Notify authorized Exchange users when an Issuer has updated any Issuer, plan and provider data	W	
NO-107	Notification	Plan Management	CGI Plan Management	CGI Plan Management.	Authorized Exchange users must automatically receive notification that an enrollment request has been received.	W	
NO-108	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Generate an electronic notification to the Insurance Division indicating the plan enrollment status upon approval of the enrollment change request.	W	
NO-109	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Approval of the enrollment change request must generate an electronic notification to Exchange issuers indicating the plan enrollment status	W	
NO-110	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Approval of the enrollment change request must generate an electronic notification to registered Navigators/Brokers indicating the plan enrollment status	W	
NO-111	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Approval of the enrollment change request must send an update transaction to the appropriate CMS system for plan management and fiscal management functions indicating the plan enrollment status change and other information required by CMS	W	
NO-112	Notification	Plan Management	CGI Plan Management	CGI Plan Management	Approval or disapproval of the enrollment change request must send notification to the requesting Issuer.	W	

Technical Requirements Traceability Matrix

TC-1	General	Non-functional	All, as appropriate	Be designed to be scalable and flexible in order to accommodate and be easily adaptable to changes required by state and/or federal statute, mandate, decision, or policy.	S	
TC-2	General	Non-functional	All, as appropriate	Be designed, built and deployed with enterprise architecture best practices including substantial reliance on highly configurable SOA components.	S	
TC-3	General	Non-functional	Oracle Policy Automation	Provide a business rules engine as specified by 42 CFR Part 433 and Section 1561 guidance to support state, federal rules, Exchange policy and be easily configurable by a trained business analyst.	S	

Technical Requirements Traceability Matrix

TC-4	General	Non-functional	Siebel	Provide a workflow engine to support the routing of work items, work queues, etc.	S	
TC-5	General	Non-functional	ThunderheadNow	Provide a electronic document management system integrated with the workflow engine to support the handling of paper documentation	W	
TC-6	General	Non-functional	All, as appropriate	Be deployable and maintainable with Service Level Agreements as defined by the Exchange and functionality to ensure operational capabilities and integrity.	S	

Technical Requirements Traceability Matrix

TC-7	General	Non-functional	All, as appropriate	Support "plain language" as defined in the Plain Language Act of 2010.	S	
TC-8	Auditing	Solution	All, as appropriate	Provide the ability to audit and log the network system/application and detailed user activity including data available to the user, data viewed by user, data downloaded by user, data uploaded by the solution, and all actions taken by user while in the system) in accordance with policy defined by the Exchange.	W	
TC-9	Auditing	Solution	All, as appropriate	Provide and retain transaction logs in accordance with the National Institute of Standards and Technology (NIST) requirements.	S	

Technical Requirements Traceability Matrix

TC-10	Auditing	Solution	All, as appropriate	Provide and retain transaction logs in accordance with the Health Insurance Portability and Accountability Act (HIPAA).	S	
TC-11	Auditing	Solution	All, as appropriate	Provide and retain transaction logs in accordance with the Harmonized Security and Privacy Framework.	S	
TC-12	Auditing	Solution	All, as appropriate	Provide reporting for security audits and compliance activities based on designated timeframes.	W	

Technical Requirements Traceability Matrix

TC-13	Auditing	Solution	All, as appropriate	Provide ability to set security controls for audit logs via role based access controls.	S	
TC-14	Auditing	Solution	All, as appropriate	Provide flexible audit report function (including on demand feature) and audit logging ability.	W	
TC-15	Auditing	Solution	All, as appropriate	Provide ability to perform the database capabilities to facilitate auditing.	S	

Technical Requirements Traceability Matrix

TC-16	Auditing	Contractor	CGI Government Cloud	The Contractor shall support an audit of data center operations by a 3rd party vendor, including, but not limited to: SSAE-16, Pentration Test, etc.	S	
TC-17	Auditing	Contractor	All, as appropriate	The Contractor shall provide the ability for the Exchange to examine system and error daily logs to minimize and predict system problems and initiate appropriate action.	S	
TC-18	Disaster Recovery	Solution	CGI Government Cloud	The Contractor shall provide the ability to utlize alternative remote back-up sites that are at least 60 miles or as agreed upon by the Contractor and the Exchange, and are separate and distinct from primary hosting vacility with a ramp up period within the Recovery Time Objective defined by the Exchange.	S	

Technical Requirements Traceability Matrix

TC-19	Disaster Recovery	Contractor	CGI Government Cloud	The Contractor shall provide the ability to reover lost or deleted data from backup in accordance with the Recovery Point Objective as defined by the Exchange.	S	
TC-20	Disaster Recovery	Contractor	CGI Government Cloud	The contractor shall provide planned outage notification within the limits defined by the Exchange.	S	
TC-21	Disaster Recovery	Contractor	CGI Government Cloud	The contractor shall provide the ability to rollover to an alternate / backup site during planned and unplanned maintenance.	S	

Technical Requirements Traceability Matrix

TC-22	Disaster Recovery	Contractor	CGI Government Cloud	The contractor shall store backed-up data apart from the production data center that are at least 60 miles or as agreed upon by the Contractor and the Exchange to prevent simultaneous loss of production and backup data stores.	S	
TC-23	Disaster Recovery	Contractor	CGI Government Cloud	The contractor shall establish an alternative recovery location for business users in the event of a significant interruption to the production system environment.	S	
TC-24	General	Solution	All, as appropriate	The solution shall provide the ability to integrate with state systems and databases to allow interoperability as appropriate with health informatino exchanges and agencies	C	CGI will provide intergration services to the appropriate exchnages and agencies in accordance with Hawai`i requirements

Technical Requirements Traceability Matrix

TC-25	General	Solution	All, as appropriate	The solution shall support multiple industry standard operation systems.	S	
TC-26	General	Solution	OneGate	The solution shall support small personal computing devices that will include the following mobile phone and tablet platforms: - iPhone - iPad - Android phones and tablets - Blackberry phones and tablets - Windows mobile phones and tablets	W	
TC-27	General	Solution	All, as appropriate	The solution shall comply with Centers for Medicaid and Medicare Services (CMS) requirements to establish a framework of enabling technologies and processes that support improved administration of the Medicaid program, in accordance with the MITA 3.0 framework.	S	

Technical Requirements Traceability Matrix

TC-28	General	Solution	All, as appropriate	The solution shall offer a modular, flexible approach to systems development using MITA 3.0 guidelines and SOA component-oriented design principles.	S	
TC-29	General	Solution	All, as appropriate	The solution shall allow for the alignment with and increasing advancement of Medicaid Information Technology Architecture (MITA) maturity for business, architecture, and data in all systems development efforts.	S	
TC-30	General	Solution	All, as appropriate	The solution shall meet ADA and LEP requirements set by the ACA	S	

Technical Requirements Traceability Matrix

TC-31	General	Solution	ThunderheadNow	The solution shall provide the ability to receive, store, display, and print documents sent to the Exchange.	S	
TC-32	General	Contractor	All, as appropriate	The contractor shall ensure that the solution and Service Center complies with all applicable State Information Security Policy (Rev. November 13, 2009).	W	
TC-33	General	Contractor	All, as appropriate	The contractor shall provide a method to test the solution compliance against Section 508(c) of the Rehabilitation Act for all types of user interface screens (static, dynamic, Web, client-server, mobile, etc.).	S	

Technical Requirements Traceability Matrix

TC-34	Hosting Services	Solution	All, as appropriate	The solution shall provide the ability to support commonly used Internet browsers with backwards compatability as defined by the Exchange.	S	
TC-35	Hosting Services	Solution	CGI Government Cloud	The solution shall utilize a service management framework such as ITIL v3 or equivalent framework to manage IT services and infrastructure.	S	
TC-36	Hosting Services	Solution	CGI Government Cloud	The solution must include hosting services for the development, testing/verification, training, certification and production environments that will be used to develop, maintain, and operate the solution.	S	

Technical Requirements Traceability Matrix

TC-37	Hosting Services	Solution	All, as appropriate	The solution shall provide a standardized mechanism for Conflict Management and data integrity.	S	
TC-38	Hosting Services	Solution	CGI Government Cloud	The solution shall be hosted in an environment that ensures that servers are housed in a climate-controlled environment that meets industry standards including, fire and security hazard detection, electrical needs, and physical security.	S	
TC-39	Hosting Services	Solution	All, as appropriate	The contractor shall provide the ability for the state to examine system and error logs daily to minimize and predict system problems and initiate appropriate action.	S	

Technical Requirements Traceability Matrix

TC-40	Hosting Services	Solution	All, as appropriate	The contractor shall completely test and apply patches for all third-party software products before release.	S	
TC-41	Hosting Services	Solution	Maintenance and Operations Support	The Contractor shall notify the Exchange prior to the application of any testing or application of moedifications to third-party software products	S	
TC-42	Hosting Services	Solution	CGI Government Cloud	The contractor shall ensure that non-critical system management, virtualization, and administrative operational and system administration controls are isolated on the network layer that would contain protected health information (PHI) to prevent unnecessary administrative access to PHI.	S	

Technical Requirements Traceability Matrix

TC-43	Hosting Services	Solution	CGI Government Cloud	The system shall utilize industry standard security protocols for transmitting data over networks (e.g. SSL, TLS, etc.)	S	
TC-44	Hosting Services	Solution	CGI Government Cloud	The contractor shall implement network protection capabilities to detect and eliminate malicious software and/or unauthorized external connection attempts on network monitoring devices, servers, peripheral devices, and desktop workstations.	S	
TC-45	Hosting Services	Contractor	CGI Government Cloud	The contractor shall provide all hosting services at data center(s), including back-up and recovery, at sites located within the United States.	S	

Technical Requirements Traceability Matrix

TC-46	Hosting Services	Contractor	CGI Government Cloud	The contractor shall ensure that all data center operations and technical staff shall be located within the United States.	S	
TC-47	Hosting Services	Contractor	CGI Government Cloud	The contractor is required to host, maintain, and operate the solution in production for the contract term.	S	
TC-48	Hosting Services	Contractor	CGI Government Cloud	The contractor will be responsible for providing, installing, and maintaining all hardware, software, network components, and other infrastructure elements for the solution.	S	

Technical Requirements Traceability Matrix

TC-49	Hosting Services	Contractor	Maintenance and Operations Support	The contractor shall maintain reliable business operations in accordance with the agreed upon SLA.	S	
TC-50	Hosting Services	Contractor	Maintenance and Operations Support	The Contractor shall provide a system with response times and transaction volume as defined by agreed upon SLA.	S	
TC-51	Identity Management and Authentication	Solution	Oracle Identity Management	The system will enforce a single system identify for each unique user involved with the Exchange	S	

Technical Requirements Traceability Matrix

TC-52	Identity Management and Authentication	Solution	Oracle Identity Management	The solution will be able to establish family or household linkages between individual accounts.	S	
TC-53	Identity Management and Authentication	Solution	CGI Government Cloud	The solution shall provide intrusion detection and prevention services.	S	
TC-54	Identity Management and Authentication	Solution	CGI Government Cloud	The solution shall provide Certificate Authority for secure server side transactions.	S	

Technical Requirements Traceability Matrix

TC-55	Identity Management and Authentication	Solution	Oracle Identity Management	The solution shall provide a complete user provisioning and de-provisioning solution to support achievement of the privacy and security requirements as defined by the Exchange.	S	
TC-56	Identity Management and Authentication	Solution	Oracle Identity Management	The solution shall support user account authenticaion procedures with configurable parameters (time, cipher strength, logon attempts, etc.).	S	
TC-57	Identity Management and Authentication	Solution	Oracle Identity Management	The solution shall support account retirement and deactivation requirements as determined by Exchanbe identity management policies and procedures.	S	

Technical Requirements Traceability Matrix

TC-58	Identity Management and Authentication	Solution	Oracle Identity Management	The solution shall support issue and manage public key certificates for secure transactions.	S	
TC-59	Identity Management and Authentication	Solution	Oracle Identity Management	The solution shall support the ability to verify and validate system identity via public key certificates for secure transactions.	S	
TC-60	Identity Management and Authentication	Solution	Oracle Identity Management	The solution shall support the ability to delegate or utilize 3rd party authentication services for specific transactions via an external trust and authentication	S	

Technical Requirements Traceability Matrix

TC-61	Information Technology Help Desk	Contractor	CGI Government Cloud	The Contractor shall provide live Tier-1 support 24X7.	S	
TC-62	Information Technology Help Desk	Contractor	Maintenance and Operations Support	The Contractor shall be held accountable to issue resolution standards as defined by the agreed upon SLA.	S	
TC-63	Information Technology Help Desk	Contractor	CGI Government Cloud	The Contractor shall operate and incident management system that provides reporting in line with agree upon SLA.	W	

Technical Requirements Traceability Matrix

TC-64	Interfaces	Solution	All, as appropriate	The solution shall provide real-time interfaces to transfer data between the Exchange's solution and existing state systems (such as the Eligibility Rules Engine, state Medicaid systems, Case Management systems, Identity Access Management systems, SERFF, HIOS, Federal Data Services Hub, etc.), databases and financial systems.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
TC-65	Interfaces	Solution	All, as appropriate	The solution shall provide new and or update existing two-way, real-time interfaces to transfer data between the system and 3rd party vendors (i.e. Insurance Division, insurance carriers, federal databases, etc).	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
TC-66	Interfaces	Solution	All, as appropriate	The solution shall provide interfaces to existing State systems that leverage existing interface designs to incorporate extensible markup language (XML) to support the requirements of the solution and associated applications.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.

Technical Requirements Traceability Matrix

TC-67	Interfaces	Solution	Oracle Enteprise Service Bus	The solution shall provide functionality that knows how, and when, to communicate with interfacing systems.	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
TC-68	Interfaces	Solution	All, as appropriate	Provide flexiblility to interface using industry standard protocols (e.g. XML, 5010, etc.)	C	CGI will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.
TC-69	Maintenance and Operations	Contractor	Maintenance and Operations Support	The contractor shall provide routine maintenance periods as defined by the agreed upon SLA.	S	

Technical Requirements Traceability Matrix

TC-70	Maintenance and Operations	Contractor	Maintenance and Operations Support	The contractor shall conduct non-routine maintenance during a mutually agreeable timeframe as defined by the agreed upon SLA.	S	
TC-71	Maintenance and Operations	Contractor	Maintenance and Operations Support	Conduct testing on any changes,upgrades to hardware or patches applied to ensure backward compatibility of its solution and integration within and outside the Exchange	S	
TC-72	Maintenance and Operations	Contractor	Maintenance and Operations Support	The contractor shall work with the Exchange team in advance of any release or changes to allow the Exchange team to adequately test, verify and train to support the smooth operation of the Exchange and its solutions	S	

Technical Requirements Traceability Matrix

TC-73	Maintenance and Operations	Contractor	Maintenance and Operations Support	Provide access for appropriate and authorized Exchange team members to the test and training environments to ensure correct implementation of changes before the changes are released to the production environment	S	
TC-74	Maintenance and Operations	Contractor	Maintenance and Operations Support	Provide version control management capability. All changes to the solution shall be reported and approved by the state, be maintained in the Contractor's version control management solution, which shall be available to the Exchange for review and audit as needed.	S	
TC-75	Regulations & Statutory Compliances	Solution	All, as appropriate	The solution shall ensure The solution meets hosting and handling standards Payment Card Industry (PCI) and ACH data.	C	The Hawai`i Exchange solution will meet applicable regulations

Technical Requirements Traceability Matrix

TC-76	Security	Solution	All, as appropriate	The solution shall comply with industry standards and regulations to include, but not limited to the following: Privacy and transaction standards, Federal civil rights laws, Standards adopted by the Secretary under Section 1104 of the Affordable Care Act (ACA), Standards and protocols adopted by the Secretary under Section 1561 of the ACA including NIST SP 800-52, 800-53i, 800-77, or 800-113 or others as specified in the federal	W	The Hawai`i Exchange solution will meet applicable regulations
TC-77	Security	Solution	CGI Government Cloud	The solution shall support penetration testing from external vendors.	S	
TC-78	Security	Solution	CGI Government Cloud	The solution shall maintain strict access controls to safeguard all areas where Exchange data could be accessed.	S	

Technical Requirements Traceability Matrix

TC-79	Security	Solution	CGI Government Cloud	The sholution shall implement correct plans from internal and external risk assessment and vulnerability testing and/or external (3rd Party) HIPAA audit/review that discusses thrests, vulnerabilities and impacts, including network and web application.	S	
TC-80	Security	Solution	Oracle Identity Management	The solution shall implement a provisiong, review, and de-provisioning scheme for user identification, authentication and authorization, including activation and de-activation.	S	
TC-81	Security	Solution	Oracle Identity Management	The solution shall manage user profiles including defining access to data types and security credentials.	S	

Technical Requirements Traceability Matrix

TC-82	Security	Solution	Oracle Identity Management	The solution shall allow users to reset passwords and unlock locked accounts from a web portal interface.	S	
TC-83	Security	Solution	Oracle Identity Management	The solution shall pass credentials for authentication and authorization from the Exchange solution to authenticate system access to web service transactions.	S	
TC-84	Security	Solution	Oracle Identity Management	The solution shall restrict access to user, provider, or organizational data to authorized users.	S	

Technical Requirements Traceability Matrix

TC-85	Security	Solution	Oracle Identity Management	The solution shall ensure non-repudiation* as part of digital signature verification to prevents data from being altered, deleted or damaged during exchange.	S	
TC-86	Security	Solution	Oracle Identity Management	The solution shall have the ability to set automatic alerts to system administrators when a breach pattern or unauthorized use activity is detected.	S	
TC-87	Security	Solution	All, as appropriate	The solution shall support "user exits" or a "pluggable authentication module" (PAM) to enable user transition between the solution and local systems that are authorized as third party connections to the solution.	S	

Technical Requirements Traceability Matrix

TC-88	Security	Solution	Oracle Identity Management	The solution shall implement and support two-factor authentication (i.e. two kinds of evidence).	W	
TC-89	Security	Solution	All, as appropriate	The solution shall provide the ability for web service providers and service consumers to interact via the solution.	S	
TC-90	Security	Solution	All, as appropriate	The solution shall provide the ability to implement security for transport and messaging via web services.	S	

Technical Requirements Traceability Matrix

TC-91	Security	Solution	All, as appropriate	The solution shall track all access so that an Accounting Of Disclosures report can be provided to the individual if requested.	S	
TC-92	Security	Solution	All, as appropriate	The solution shall provide the ability disable accounts as defined in the agreed upon SLA.	S	
TC-93	Security	Solution	All, as appropriate	The solution shall provide security administration functionality to apply user permissions based on roles to accommodate access controls that align with federal (ANSI) standards for Role Based Access Controls.	S	

Technical Requirements Traceability Matrix

TC-94	Security	Solution	All, as appropriate	The solution shall ensure that all health information in transit and at rest is unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified by the Secretary of the Federal Department of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5) , or any update	W	
TC-95	Security	Solution	All, as appropriate	The solution shall provide the same security provisions for the development, system test, acceptance test and training environment as those used in the production environment.	S	
TC-96	Security	Contractor	All, as appropriate	The contractor shall ensure that the Exchange solution system documentation is protected from unauthorized access.	S	

Technical Requirements Traceability Matrix

TC-97	Security	Contractor	Oracle Identity Management	The Contractor shall define all initial user security roles and access permissions as defined by the State to ensure users are able to access the system at system go-live.	W	
TC-98	Training	Contractor	Maintenance and Operations Support	The Contractor shall provide initial and ongoing maintenance and operations training for State and Exchange staff.	W	

Web Portal UX Requirements Traceability Matrix

WP-1	Web Portal	Design	OneGate	OneGate	Design based on Enrollment 2014 UX project	S	vermonthealthconnect.gov - ne URL. Info now. Template works for now. New space. Info site no - transactional later. RFP was fo OneGate and the info site. Some look and feel still could be used. Wanted a UX group to think thr it. GMMB put together the content. Next three weeks will have the info site up. Need help defining the user experience - persona's etc. Want from Exeter what can be changed in the UX OneGate versus cannot. Logo.
WP-2	Web Portal	Design	OneGate	OneGate	Provide content specific help on screen for users	S	
WP-3	Web Portal	Design	OneGate	OneGate	Provide additional language support featues. At a minimum, the system should provide language "flag" icons to direct consumes in their native language to Navigator and/or Translation services	S	
WP-4	Web Portal	Design	Siebel Public Sector CRM	Siebel Public Sector CRM	Persist live chat and telephone support options on all Portal views	W	
WP-5	Web Portal	Design	OneGate	OneGate	Provide trained business user portal content management capabilities	S	
WP-6	Web Portal	General	OneGate	OneGate	Display general information about the state's health and human services programs publicly for all users to view without requiring a login.	S	

Web Portal UX Requirements Traceability Matrix

WP-7	Web Portal	General	OneGate	OneGate	Display and provide browsing capabilities on the various health options and plans available to users without requiring a login.	S	
WP-8	Web Portal	General	OneGate	OneGate	Provide robust search capability for information contained on the portal without requiring a login.	S	
WP-9	Web Portal	General	OneGate	OneGate	Provide capability for users to search for Navigators using a variety of criteria without requiring a login.	S	
WP-10	Web Portal	General	OneGate	OneGate	Provide information on the procedures, including materials that will be needed to complete the application process for signing up for health coverage without requiring a login.	S	
WP-11	Web Portal	General	OneGate	OneGate	Provide users (including authorized representatives) the option to complete a pre-screening of potential eligibility for state health and human services programs via a configurable module.	S	
WP-12	Web Portal	General	OneGate	OneGate	Provide an expedited expert level pre-screening function to Navigators, brokers, call center staff, and caseworkers.	S	
WP-13	Web Portal	General	OneGate	OneGate	Accept input from Navigators, caseworkers, Call Center staff and customers necessary for pre-screening.	S	
WP-14	Web Portal	General	OneGate	OneGate	Display the results of the pre-screening assessment of eligibility to Navigators, caseworkers, call center staff, and customers.	S	

Web Portal UX Requirements Traceability Matrix

WP-15	Web Portal	General	OneGate	OneGate	Provide the ability to flag any information or situations that require more detailed information and direct individuals for further assistance.	W	
WP-16	Web Portal	General	OneGate	OneGate	Support additional data-gathering regarding user experience with QHPs and/or quality of care (i.e. surveys, questionnaires, etc.)	S	
WP-17	Web Portal	Identity	OneGate	OneGate	Provide unverified exchange web portal login/accounts - Enable user to save information and return to the site without giving 'official' identity verification data (e.g. SSN, name, etc)	S	
WP-18	Web Portal	Identity	OneGate	OneGate	Provide verfied Exchange web portal login/accounts with appropriate system access according to system assigned role (e.g. consumer, Navigator, Issuer, etc.) - Verified accounts are those for whom the individual identity has been verified through an authoritative source (i.e. SSN validation)	S	
WP-19	Web Portal	Enrollment	OneGate	OneGate	Enable individual users to self declare income information for use in plan comparison. Persist this information for later sessions if the user has created an Exchange Web Portal account	S	

Web Portal UX Requirements Traceability Matrix

WP-20	Web Portal	Enrollment	OneGate	OneGate	Enable individual users to compare plans based on factors such as: - Price/premium payment - Deductible - Medal Rating (bronze, silver, gold, platinum) - Quality assessment - Provider availability - Benefit structure - Product Type (e.g. Vision, Dental, etc.) - Membe-provided feedback rating	S	
WP-21	Web Portal	Enrollment	OneGate	OneGate	Provide multiple summary and detail levels of plan comparison information	S	
WP-22	Web Portal	Enrollment	OneGate	OneGate	Enable users to look up the providers that are affiliated with specific plans and affiliation type (i.e. Tiered PPO model).	W	
WP-23	Web Portal	Enrollment	Plan Management	Plan Management	Provide ability for Issuers to upload supporting documentation to the plan selection tool	W	
WP-24	Web Portal	Enrollment	OneGate	OneGate	Provide a plan selection recommendation engine or wizard that can filter initial results based upon additional user preference and input.	S	
WP-25	Web Portal	Enrollment	OneGate	OneGate	Provide capability for users to download additional supporting plan documentation as provided by the Issuer	S	
WP-26	Web Portal	Enrollment	OneGate	OneGate	Provide calculator functionality for individuals to estimate their premiums including potential premium tax credit subsidies and cost sharing reductions	S	

Web Portal UX Requirements Traceability Matrix

WP-27	Web Portal	Eligibility	OneGate	OneGate	Provide a dynamic application entry engine to collect information required to determin eligibiltiy for health and human service programs. The system shall tailor the application process based upon user response to questions.	S	
WP-28	Web Portal	Eligibility	OneGate	OneGate	Provide a progress bar to show users where they are in the application process	s	
WP-29	Web Portal	Eligibility	OneGate	OneGate	Enable individual users to submit information for eligibility, for example: - SSN - Address - Date of birth - Name - Household income	S	
WP-30	Web Portal	Eligibility	OneGate	OneGate	Provide status of eligibility request received from the eligibility service	C	CGI will develop the necessary interfaces, using the ESB, with th Federal and State Agencies as necessary to comply with ACA requirements.
WP-31	Web Portal	Eligibility	OneGate	OneGate	Display eligibility results received from the eligibility service	C	CGI will develop the necessary interfaces, using the ESB, with th Federal and State Agencies as necessary to comply with ACA requirements.
WP-32	Web Portal	Eligibility	OneGate	OneGate	Enable individual users to apply for benefits eligibility using alternate income verification (i.e. paper verification).	W	

Web Portal UX Requirements Traceability Matrix

WP-33	Web Portal	Enrollment	OneGate	OneGate	Enable individual users to enroll in a plan which they have selected	S	
WP-34	Web Portal	Enrollment	OneGate	OneGate	Enable indivdiual users to reenroll (renew) in a plan which they have selected	S	
WP-35	Web Portal	Financial Management	OneGate	OneGate	Allow users to set up payment options for their selected plan(s)	S	
WP-36	Web Portal	Financial Management	OneGate	OneGate	Allow users to make recurring and scheduled electronic premium payments through the Exchange portal	S	
WP-37	Web Portal	Financial Management	OneGate	OneGate	Allow authorized users the ability to view their payment histories on the Web Portal	W	
WP-38	Web Portal	Small Business	OneGate	OneGate	Enable Employer to set up SHOP plan selection(s)	S	
WP-39	Web Portal	Small Business	OneGate	OneGate	Enable Employees to compare available SHOP plans	S	
WP-40	Web Portal	Small Business	OneGate	OneGate	Enable Employees to enroll or unenroll in SHOP plan	S	
WP-41	Web Portal	Small Business	OneGate	OneGate	Allow employers to set up payment options for premiums	W	
WP-42	Mobile Web Portal	Enrollment, Financial Management	OneGate	OneGate	Enable users of all plans to view their enrollment and payment status, plan details, and notification history	S	
WP-43	Mobile Web Portal	Eligibility	OneGate	OneGate	Enable users to upload eligibility documents using their camera equipped mobile device	S	
WP-44	Support Intranet	Security	OneGate	OneGate	Provide role based access to Exchange Portal content	S	
WP-45	Web Portal	Administration	OneGate	OneGate	Provide role based portal administration function	S	

Web Portal UX Requirements Traceability Matrix

WP-46	Web Portal	Financial Management	OneGate	OneGate	View Invoice and invoice details for Individual, Employer and Issuers	S	
WP-47	Web Portal	Financial Management	OneGate	OneGate	Make electric payment for Individual, Employer, and Issuer	S	
WP-48	Web Portal	Financial Management	OneGate	OneGate	View notification history for Individuals, Employers, and Employees	S	
WP-49	Web Portal	User Customization	OneGate	OneGate	Provide customizable portal views and functionality based on user role for "super users" (e.g. Navigator, Broker, caseworker, etc.)	S	
WP-50	Web Portal	User Customization	OneGate	OneGate	Provide a dashboard of key information and metrics for "super users" including electronic notice posting area.	W	
WP-51	Web Portal	User Customization	OneGate	OneGate	Allow TPAs/QHP issuers to access the Exchange through a customized portal in order to add, manage, certify, recertify, and delete their health plans.	W	
WP-52	Web Portal	User Customization	OneGate	OneGate	Allow SHOP owners access to the Exchange through a custom portal and add or manage health plan options for their employees.	S	
WP-53	Web Portal	User Customization	OneGate	OneGate	Allow SHOP employees to access a custom portal where they can view and select among their plans options, enroll their family and manage changes in circumstances.	S	

Consumer Assistance - General Requirements Traceability Matrix

CAG-1	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system must support the complaints/appeals process.	W	
CAG-2	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall allow customer support representative to log customer complaints and appeals.	W	
CAG-3	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall allow staff to attach relevant documents to complaint or appeal.	S	
CAG-4	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	Associated recorded calls/transcripts and online chat sessions log with the appropriate appeal	W	
	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall prompt customer support representative on complaints/appeals workflow by integrating with workflow/document management system.	W	existing manual interact with th Training issue or other approach Maximus - trust in their training capacity. Validating ID is the largest issue. Co-browsing - wal a person thru enrollment. Implementation issues.
CAG-6	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system will track time frames and deadlines for responding to complaints and appeals.	W	
CAG-7	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall allow customer support representative to generate letters to consumer throughout appeals/complaints process.	W	Thunderhead would be good. Must have State approve forms Author, edit, publish. Bias to outsource the work. Current - p from ACCESS, generate labels, print and mail, repost. Ideal
CAG-8	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall track complaint or appeal throughout process so that specified Complaints/Appeals staff can view status, see where it is in process and report back to consumer at any time.	W	

Consumer Assistance - General Requirements Traceability Matrix

CAG-9	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall support the process for sending appeals/complaints to be reviewed by appropriate parties within and outside the State and recording decisions, adding documentation, etc.	W	
CAG-10	Consumer Assistance	Complaints / Appeals	OneGate	OneGate	The system shall allow enrollment, coverage, and tax credits to be changed as a result of a complaint/appeal decision.	S	
CAG-11	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall allow appeals/complaints staff to manage cases within the system using options including tickler files, response and review dates, document management, email, and fax.	W	% appeal work to overall is sma under 2500 over a year. Grow future, but still small. Post note in ACCESS. Appealing data in th hub is a concern. Maybe handl thru a generic "case". Live with generic and learn for future.
CAG-12	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall allow consumers to submit complaint/appeal via phone, web, chat session, email, and letter.	S	Do not take HIPPA data thru ch and email. Documentation is phone, mail, and in person.
CAG-13	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall provide options to secure complaints/appeals for confidentiality reasons (e.g. hide consumer name) and allow access to cases by specified consumer support staff.	W	
CAG-14	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall monitor appeals/complaints due dates and alert staff or management of overdue status.	W	

Consumer Assistance - General Requirements Traceability Matrix

CAG-15	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall have the ability to be used by multiple agencies for appeals/complaints, including at a minimum the Exchange, Medicaid, and the Department of Human Services.	S	
CAG-16	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall have the ability to assign a priority, or level to the appeal/complaint.	S	
CAG-17	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The shall provide the capability to report complain and appeals data in real time and on a historical	S	
CAG-18	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall provide notifications to the appropriate parties upon the following key events in the complaint/appeal process: - Reciept of complaint/appeal - Status Change - Resolution	W	
CAG-19	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall support outreach initiatives using letters, emails, phone calls, text messages as described below.	W	consider review of the communication approaches that cannot be documented and maintained. Chat - January, not October.
CAG-20	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall ask and store consumers' preferred method of communication.	W	Should be in. Outbound communication preferences.
CAG-21	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall provide consumers with reminders to update their circumstances and renew eligibility for subsidies/assistance, enroll in coverage, etc.	W	

Consumer Assistance - General Requirements Traceability Matrix

CAG-22	Consumer Assistance	Outreach / Education	OneGate	OneGate	The system shall generate communication to consumers regarding any relevant updates or information to health care policy or laws in their state, tips on using the web, how to find a Navigator, and other consumer assistance services.	W	
CAG-23	Consumer Assistance	Outreach / Education	OneGate	OneGate	The system shall support multi-lingual communication in at least the languages specified by the Exchange, and must be able to support additional language (including languages that use non-Western scripts).	W	In bound calls, need to be able t pull in a person (IVR - flow chart for how this would work)
CAG-24	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall log and store materials about outreach and education events across the state and community to inform the CRM and call center staff.	S	Public - massive archive for lots things so that it could be reviewed. Maximus - not archiving, store and destroy, record and monitor - coach thru training. Review later - storage needs to have a standard operating guide: lock box, etc. Document management solutio within Siebel?
CAG-25	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall collect and report on call center metrics for the purposes of identifying outreach and education opportunities	S	
CAG-26	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall collect and report on website usage metrics indcluding standard analytic metrics	S	

Consumer Assistance - General Requirements Traceability Matrix

CAG-27	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall collect and report on user demographics as feasible from web and call center interactions for the purposes of informing education and outreach activities	S	Between the website and the call center - capture demographics and user ID to customize / analytics - hit on v-farm and uptick on the call center. Exchange website may need it's own analytics. Subsets of the call information. Collecting different than reporting on it. May be specific timeframes for "turning on" the analytics.
CAG-28	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall collect and report on Navigator web and call center interactions for the purposes of informing education and outreach opportunities.	S	Same type of concerns as CAG-27. What does the reporting look like. Not in October.
CAG-29	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall flag consumer assistance staff or Navigators of relevant outreach and education materials available when consumer calls about a certain issue/inquiry.	S	
CAG-30	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall provide the functionality to generate random surveys to consumers via online, email, letter or phone and then compile data to assess consumer satisfaction.	S	
CAG-31	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall capture information on outreach efforts (e.g. how did you hear about us?).		

Consumer Assistance - General Requirements Traceability Matrix

CAG-32	Consumer Assistance	Workflow	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall improve collaboration and workflow driven processes among staff by integrating CRM with workflow, document management and document imaging technology	W	
CAG-33	Consumer Assistance	Workflow	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall have the ability to integrate voice and electronic transactions into a single workflow.	S	Record voice approval for third party - navigator to build and then the person records their approval. Do call monitoring. Challenge on policy - authority and process documentationatio Electronic - e-signature process.
CAG-34	Consumer Assistance	Workflow	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall have the ability to oversee and manage contacts through work item routing and queuing, sending online alerts to staff or supervisors if issues are high priority or overdue.	W	
CAG-35	Consumer Assistance	EDM	ThunderHeadNOW	ThunderHead NOW	Support electronic document management (EDM) capabilities	S	
CAG-36	Consumer Assistance	EDM	ThunderHeadNOW	ThunderHead NOW	The system shall provide the ability to upload attachments to all indivdiual and correspondence records.	S	
CAG-37	Consumer Assistance	EDM	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall provide the ability to view related correspondence records from a single correspondence record.	S	

Consumer Assistance - General Requirements Traceability Matrix

CAG-38	Consumer Assistance	EDM	ThunderHeadNOW	ThunderHead NOW	The system shall provide standard letter templates and the ability to add free form text to customize a letter to the customer's specific issue.	W	There may be an interest in turning on features after implementation stages. Function for turning on these items. Ways to bundle the features for schedule for training? Tina should be involved in these training expectations.
CAG-39	Consumer Assistance	EDM	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall link scanned images to correspondence and records to provide one view of all related material (images, letters, or contacts with staff).	W	
CAG-40	Consumer Assistance	Contact Tracking	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall assign a unique number to identify each instance of a contact.	S	
CAG-41	Consumer Assistance	Contact Tracking	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall accommodate the receipt and tracking of requests or inquiries via telephone, letter, fax, walk in, email, web, or any other channel used by the consumers.	S	
CAG-42	Consumer Assistance	Contact Tracking	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall track and search on contacts with basic identifying information such as time and date of contact, Provider number, member number, caller name, agent id, contact type, reason, status of issue, or any combination thereof.	W	
CAG-43	Consumer Assistance	Reporting	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall generate ad-hoc and standard reports in real time as well as historical for incoming and outgoing contacts.	S	

Consumer Assistance - General Requirements Traceability Matrix

CAG-44	Consumer Assistance	Reporting	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall report on multiple data points: volume of contacts, by contact type, reason for contact, type of consumer, complaints, appeals, resolution, transfers to other programs, consumer satisfaction, by agent, specified time frames.	S	
CAG-45	Consumer Assistance	Reporting	Siebel Public Sector CRM	Siebel Public Sector CRM	The system shall have the ability to extract data in user friendly formats, such as Excel.	S	
CAG-46	Consumer Assistance	Quality Monitoring	Call Center	Call Center	The system shall provide quality monitoring tools and processes to enable a continuous improvement cycle for the contact center staff that includes: - Plug-in - Silent monitoring (including remote) - Record and review to assess whether call was answered accurately - Voice and screen/multi-media monitoring - Conferencing capabilities - Ability to assess or rate an agent's quality and service using grading system and to store that data	O	CGI assumes that quality monitoring of calls will occur within the call center tools. Decision needs to be made: Deliverable of a plan about CTI. Don't do Quality monitoring for now (or just with what's available). Scope tool to manage the vendor.

Consumer Assistance - Case Management Requirements Traceability Matrix

CACM-1	Consumer Assistance	Case Management	OneGate	OneGate	Provide the ability to add multiple dated narratives to a case and track and maintain changes over time via the narratives.	W	Ecosystem and escalation points need to be identified for the CRM, part of the Gap Analysis activity. SOV may review with Maximus for additional feedback. KPMG - one or a few sessions - current mapping, escalation and role and future state. General likelihood is that push more into Maximus. Leaky system currently within state. Might inform other work streams (like premium processor). If some things known, like
CACM-2	Consumer Assistance	Case Management	OneGate	OneGate	Maintain a history of notices that have been sent to a individual, employer, Navigator, Broker.	W	
CACM-3	Consumer Assistance	Case Management	OneGate	OneGate	Maintain and a history of a individual's eligibility status over time.	S	

Consumer Assistance - Case Management Requirements Traceability Matrix

CACM-4	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and Customer Support staff to modify the eligibility/enrollment record to indicate beginning and ending dates of coverage and specify the program or product for which the individual is eligible.	S	
CACM-5	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and Customer Support staff to deactivate a particular customer's case.	S	
CACM-6	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and Customer Support staff shall to reactivate a client's case based on new information, new application or redetermination.	S	
CACM-7	Consumer Assistance	Case Management	OneGate	OneGate	Provide mechanism to check and flag duplicate individual cases.	W	
CACM-8	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and Customer Support staff to merge (and un-merge) multiple individual cases.	W	
CACM-9	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkersand Customer Support staff to mark a case duplicate, but remain unmerged.	S	
CACM-10	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and customer support staff the ability to search for a specific individuals's information.	S	
CACM-11	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and Customer Support staff to view individual information.	S	
CACM-12	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and Customer Support Staff to add to a individual's information.	S	
CACM-13	Consumer Assistance	Case Management	OneGate	OneGate	Allow Caseworkers and Customer Support Staff to change or modify an individual's information.	S	

Consumer Assistance - Case Management Requirements Traceability Matrix

CACM-14	Consumer Assistance	Customer Application Intake Process	OneGate	OneGate	Allow Caseworkers and Customer Support staff to search for the individual's eligibility details.	S	
CACM-15	Consumer Assistance	Customer Application Intake Process	OneGate	OneGate	Allow Caseworkers and Customer Support Staff to view the individual's eligibility details (e.g., income sources, citizenship, immigration status, etc.).	S	
CACM-16	Consumer Assistance	Customer Application Intake Process	OneGate	OneGate	Allow Caseworkers and Customer Support staff to add new data into the individual's eligibility details (income sources, citizenship, immigration status, etc.).	S	
CACM-17	Consumer Assistance	Case Management--Administration	OneGate	OneGate	Provide a mechanism for role-based access control for any changes to the rules or parameters in the rules engine.	S	
CACM-18	Consumer Assistance	Case Management--Administration	OneGate	OneGate	Track all changes made to an account in an auditable log.	W	
CACM-19	Consumer Assistance	Case Management - Administration	OneGate	OneGate	The system must provide queries/reports to track and manage complaint workload, disposition, assignments and status	W	
CACM-20	Consumer Assistance	Case Management--System Access	OneGate	OneGate	Allow supervisors to enter the system through a customized portal to view and manage all the cases of the caseworkers under their jurisdiction.	S	
CACM-21	Consumer Assistance	Case Management--System Access	OneGate	OneGate	Allow administrators to enter the system through a customized portal to view, manage, and if necessary correct case data if a computer systems error has occurred, as long as there is sufficient documentation noted in the record. Any system errors that are identified will be reviewed through a quality assurance process.	S	

Navigator Requirements Traceability Matrix

CAN-1	Consumer Assistance	Navigators	OneGate	OneGate	Provide consumers with general information regarding Navigator Program, including information regarding certification of Navigators and relationship to Exchange, Issuers, Providers and Brokers	S	Navigators and Brokers will have essentially the same functions in Vermont - same certification process.
CAN-2	Consumer Assistance	Navigators	OneGate	OneGate	Allow certified Navigators to enter the portal through a distinct login.	S	Not issue specific - can we develop a simple mechanism for calculating and paying small employers for "broker" services?
CAN-3	Consumer Assistance	Navigators	OneGate	OneGate	Allow Navigators to create an account with the Exchange.	S	able to associate navigators with exchange activity measures - have a manner to "ask" citizens if they had navigator assistance
CAN-4	Consumer Assistance	Navigators	OneGate	OneGate	Require Navigators to provide credentials and certification information to establish an account.	S	

Navigator Requirements Traceability Matrix

CAN-5	Consumer Assistance	Navigators	OneGate	OneGate	Allow consumers to see the Navigator's credentials and certification information and select a Navigator based on them. It will also flag Management if Navigator information is not up to date, or on probation for misconduct.	W	
CAN-6	Consumer Assistance	Navigators	OneGate	OneGate	Verify the information provided by the Navigator.	W	
CAN-7	Consumer Assistance	Navigators	OneGate	OneGate	Create an account for the Navigator and assign a unique ID that will be maintained in the Navigator account.	S	
CAN-8	Consumer Assistance	Navigators	OneGate	OneGate	Track the number of persons assisted by each Navigator on a monthly basis and produce detailed reports on such activity.	W	May want to expand to other measures

Navigator Requirements Traceability Matrix

CAN-9	Consumer Assistance	Navigators	OneGate	OneGate	Generate reports by Navigator; determining effectiveness by community, population, enrollment.	W	
CAN-10	Consumer Assistance	Navigators	OneGate	OneGate	Track Navigator performance metrics as defined by the state to determine effectiveness of Navigator or use incentive based compensation (e.g.., number of enrollees, referrals, problem resolution, etc.)	W	Needs some further clarification
CAN-11	Consumer Assistance	Navigators	OneGate	OneGate	Provide a feedback or communication loop to the Navigators; a way for state agencies to communicate information to them (for example, change in QHPs, new programs or processes on which they need education).	W	

Navigator Requirements Traceability Matrix

CAN-12	Consumer Assistance	Navigators	OneGate	OneGate	The system shall flag Management if Navigator has performance issues (e.g.., missing deadlines, aging and outstanding customer inquiries, incomplete applications, enrollment, etc.).	W	what are the metrics for reporting issues? Compaints, grievance etc.

Mandatory Optional Requirements Traceability Matrix

MO-1	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The CRM shall manage contacts with, including but not limited to, Providers, Members, Consumers, Navigators, Brokers and other entities as identified by the Exchange.	S	
MO-2	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system will support multimedia communications such as but not limited to: email, letter, phone, fax, web portal, chat, text messages.	S	
MO-3	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide online access to customer support staff about caller information and real-time transaction activity (e.g. application status, premium payment).	W	
MO-4	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide the ability to archive and purge calls, contacts, correspondence from the CRM according to Exchange-defined criteria.	W	
MO-5	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall have the ability to store the caller's preferred method of communication, including need for deaf or other language interpretation.	W	
MO-6	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide speech and hearing impaired customers with the ability to communicate through a Teletypewriter (TTY) or Telecommunications Display Device (TDD).	S	NA
MO-7	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The CRM solution shalls eamlessly integrated with at least the following Customer Support technology systems and needs: - Call logging and resolution tracking - External IVR - Electronic document management - Training support - Workflow management - Reporting - Quality Monitoring	W	

Mandatory Optional Requirements Traceability Matrix

MO-8	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall maintain a record of inquiry and correspondence data online, with periodic backups managed by the CRM system administrator. The call center shall be able to store record of recordings of assisted calls, in a time frame specified by the Exchange.	S	
MO-9	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide functionality that is capable of integrating with other systems, such as Enrollment/Eligibility, the web portal, the security platform of the Case Management and the Exchange.	W	
MO-10	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall be expandable in order to support multiple contact centers in separate physical locations that support different programs, including support for the Department of Human Services customer support functions.	S	
MO-11	Consumer Assistance	CRM/Call Center Functionality	CGI Troy Call Center	Siebel Public Sector CRM	The system shall have the ability to enable security around confidential consumer data allowing designated staff access.	S	
MO-12	Consumer Assistance	IVR Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system shall interface with and support the use of an external IVR system through the Department of Human Services.	C	CGI will integrate the call center with the DHS IVR.
MO-13	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide Automatic Call Distribution (ACD) capability to answer calls from customers in sequence and record and report metrics.	S	NA
MO-14	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide capability to prioritize agents by availability, skill set, language, and overflow from other queues.	S	NA
MO-15	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide virtual hold and callback features when thresholds are met for wait time to allow consumers to hang up and receive an automated call when an agent is available.	S	NA

Mandatory Optional Requirements Traceability Matrix

MO-16	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system shall have the ability to provide consumers with estimated wait time to speak with an agent and messaging that will remind consumer of other self service options, such as web site.	S	NA
MO-17	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system will allow individual contact centers to identify and set performance metrics (e.g. 3% abandonment rate, 15 second speed of answer).	S	NA
MO-18	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system will alert management and staff when service levels are not being met.	W	NA
MO-19	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system will provide a robust scheduling and forecasting component that allows management to staff call center appropriately; data provided will show peak hours, days, months.	S	NA
MO-20	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The ACD system will have the ability to monitor and provide real time reporting and forecasting software for: - Abandonment rate - Agent availability and productivity - Average speed of answer - Call length - Contact volume - Customer satisfaction - Handle time - One call resolution rate - Peak hour statistics - Identification of historical trends	S	NA
MO-21	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system shall allow authorized managers or supervisors to monitor active calls.	S	NA
MO-22	Consumer Assistance	ACD Technology	CGI Troy Call Center	Siebel Public Sector CRM	The system shall provide the capability to record all call interactions	S	
MO-23	Enrollment	Medicaid Plan Enrollment	OneGate	OneGate	Allow for real time and paper enrollment into Medicaid health plans for all eligibles (i.e., federal and state medical assistance programs such as Medicaid, CHIP)	W	

Mandatory Optional Requirements Traceability Matrix

MO-24	Enrollment	Medicaid Plan Enrollment	OneGate	OneGate	Allow Medicaid-eligibile individuals to view available plans in the plan selection module with the same level of functionality offered to individuals shopping in the commercial market	W	
MO-25	Enrollment	Medicaid Plan Enrollment	OneGate	OneGate	Provide a mechanism to determine plan assignment, defined by the DHS, if an individual fails to select a plan within the required timeframe.	W	
MO-26	Enrollment	Medicaid Plan Enrollment	OneGate	OneGate	Allow for retroactive plan enrollment based on criteria established by DHS.	W	
MO-27	Enrollment	Medicaid Plan Enrollment	OneGate	OneGate	Transmit plan selection electronically based on DHS defined criteria.	W	

State of Vermont Enterprise Architecture
Non-Functional Requirements Traceability Matrix (RTM)
Table of Contents

		Code	Description	Tab	Order		CGI Initial Review
	Table of Contents		Table of Contents	Table of Contents	1		1/24/2013
	General		Change Log for this spreadsheet.	Change Log	2		1/24/2013
			Definitions	Definitions	3		1/24/2013
	Hosting Services	H1	Data Center	H1 Data Center	4		1/24/2013
		H1A	TIA 942 Data Center Standards	H1A TIA 942	5		1/24/2013
		H2	Infrastructure	H2 Infrastructure	6		1/30/2013
		H3	Networking	H3 Networking	7		1/30/2013
		H4	Backup Recovery	H4 Backup Recovery	8		1/30/2013
		H5	Capacity & Performance Mgmt	H5 Capacity & Performance	9		1/30/2013
		H6	Configuration Management	H6 Configuration	10		1/30/2013
		H7	Release Management	H7 Release	11		1/30/2013
		H8	Monitoring Management	H8 Monitoring	12		1/30/2013
		H9	Service Continuity Management	H9 Continuity	13		1/30/2013
		H10	Refreshes and Lifecycle	H10 Refreshes	14		1/30/2013
		H11	Maintenance and Operations	H11 M&O	15		1/30/2013
		H12	Governance	H12 Governance	16		1/30/2013
		H13	Service Level Agreement	H13 SLA	17		1/30/2013
	Security/Privacy	S1	Security Summary	S1 Security Punchlist	18		1/23/2013
		S2A	General Security Tab 1	S2A General Security	19		1/23/2013
		S2B	General Security Tab 2	S2B General Security	20		1/23/2013
		S3	Federal Security	S3 Federal Security Service	21		1/23/2013
		S4A	NIST 800-53 Summary	S4A NIST 800 Series Summary	22		1/23/2013
		S4B	NIST 800-53 Details	S4B NIST 800 Series Detail	23		1/23/2013
		S5	HIPAA	S5 HIPAA	24		1/23/2013
		S6	PHI and Privacy	S6 PHI and Privacy	25		1/23/2013
		S7	IRS 1075	S7 IRS 1075	26		1/23/2013
		S8	PCI-DSS	S8 PCI	27		1/23/2013
	Solution	SLN1	Service Oriented Architecture	SLN1 SOA	28		1/30/2013
		SLN2	Audit	SLN2 Audit	29		1/30/2013
		SLN3	Business Intelligence & Extract Transform and Load (ETL)	SLN3 BI & ETL	30		1/30/2013
		SLN4	Master Data Management and Integration	SLN4 MDM & INT	31		needed
		SLN5	Interfaces	SLN5 Interfaces	32		needed
		SLN6	Medicaid Information Technology Architecture (MITA)	SLN6 MITA	33		needed
		SLN7	Rules Engine and Standards	SLN7 Rules	34		needed
		SLN8	Portal	SLN8 Portal	35		needed
		SLN9	Enterprise Content Management (ECM)	SLN9 ECM	36		needed
		SLN10	Database Management System (DBMS)	SLN10 DBMS	37		needed
		SLN11	Application Architecture	SLN11 APP Arch	38		1/26/2013
		SLN12	Useability	SLN12 Useability	39		
		SLN13	Software Requirements and useage	SLN13 Software	40		1/26/2013
		SLN14	Users of the Solution and their touch points	SLN14 Actors	41		1/28/2013

	Target Environment Review	ENV1	see Production Environments Technical Architecture Model	see visio			
		ENV2	see Non-Production Environments Technical Architecture Model	see visio			
	WAN Connectivity	WAN1	see WAN Connectivity Schematic	File: SOV WAN Network diagram 01_29_13 v3.pdf			

Date	Author	Version	Change Reference
18-Dec-2012	Eric Stephens	v0.15	Add additional requirements from Oracle Fusion Reference Architecture
18-Dec-2012	Eric Stephens	v0.16	Merge HI/CGI NFRs
19-Dec-2012	Eric Stephens	v0.17	Add hosting::governance items
19-Dec-2012	Eric Stephens	v0.18	Add SLA tab
2-Jan-2013	Eric Stephens	v0.19	Harvest previously stricken items as requirements; convert contract-like language to requirements
2-Jan-2013	Eric Stephens	v0.20	Naming and categoriziation changes
3-Jan-2013	Eric Stephens	v0.21	Separate catagories into tabs
11-Jan-2013	Eric Stephens	v0.24	Move functional requirements to functional tab; add tab for candidate NFRs from Fx sheet and reviewed to see which were fx v. nfr. Reviewed Gartner tabs with additional requirements and consolidated.
14-Jan-2013	Eric Stephens, Rob Tornai, Rick Ketcham	v0.25	consolidate categories/tabs, final review of non-Gartner NFRs. Separate Functional requirements
15-Jan-2013	Eric Stephens	v1.0	Baseline. Add security punchlist tab, remove functional requirements tabs and redistributed to functional folks
18-Jan-2013	Eric Stephens	v1.1	Add interfaces, data conversion, and hosting environments
18-Jan-2013	Eric Stephens	v1.2	Add PCI as requirement in punchlist, add PCI tabs
18-Jan-2013	Eric Stephens	v1.3	Add IRS 1075 Tab and individual requirements from IRS document
18-Jan-2013	Eric Stephens	v1.4	Add Additional IRS 1075 to IRS 1075 tab
21-Jan-2013	MMOREY	v1.5	24 hours of cleanup. Ready for Chris Tanguay review on hosting and security
23-Jan-2013	MMOREY	V1.6	Hosting and Solution Cleanup
25-Jan-2013	MMOREY	V2.0	CGI Feedback on H1A, S1, S2A, S2B, S3, S4A, S4B, S5, S6, S7, S8 included
26-Jan-2013	MMOREY	V2.1	Added Network WAN Schematic to TOC, SLN11 added Onegate, Thunderhead, Rightfax useage, Added SLN14 Actors (Trying to clarify what Actors interact with External DMZ, WAN, External Services versus Internal Services), CGI Feedback on SLN13 and SLN11
31-Jan-2013	MMOREY	V3.0	update all hosting sheets (H2-H13) from CGI feedback and approval(Eddy P.), updates SLN1-3 from CGI approval (Matt K.) Added modified(clearer) Interface NFR Sheet (SLN5 Interfaces), Added CGI comments to Actors SLN14. Add CMS Security Documentation required for CMS per CGI.

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

	Definitions	
	Access Management	Access Management means the management of End User access to the Environments.
	Actuate Report Server	Actuate Report Server means the software of that name that is installed on a Windows Server in accordance with the Certified Configuration for Siebel CRM Programs for reporting and printing purposes.
	Administration Service	Administration Services mean Application Management Services delivered by hosting provider under an defined deployment model.
	Administrative User	Administrative User means an End User assigned by Customer to (i) identify the End Users permitted to use certain components of the hosted Environment and, (ii) to assign one or more responsibilities to each End User.
	After-Action Review	After-Action Review means the meeting held between Hosting Provider and Customer after Production Go-Live of a migration or Transition to Hosting Services for the purpose of assessing the success of the project and any outstanding issues.
	Anticipated Peak Workload	Anticipated Peak Workload means target or goal workload for the Hosting Environment during testing.
	Application Administrator	Applications Administrator means the role assigned to an End User under which such End User is responsible for performing as technical lead administrator.
	Application Management Services	Application Management Services means services performed by Hosting Provider to manage, monitor and administer the Programs within Customer's Environments.
	Application Tier	Application Tier means the server that resides in a middle-tier, between the desktop clients and the database tier. Desktop clients send their requests to a server in the Application Tier, which processes the request or sends it to another server, such as the database server. (Web Server, Forms Server, Concurrent Processing Server, Reports Server, Admin Server, etc.)
	Approved Third Party Software	Approved Third Party Software means Third Party Software separately acquired by Hosting Provider or Customer that adheres to Hosting Providers integrations and Operational standards
	Architecture Design Document	Architecture Design Document means a document prepared by Hosting Provider that specifies Customer's Hosted architecture(Physical and Logical) at the commencement of Hosting Services.
	Architecture Document	Architecture Document means a document(s) prepared and maintained by Hosting Provider that reflects the configuration of Customer's Environment during the performance of Hosting Services.
	Authorized Network Provider (ANP)	Authorized Network Provider means a network provider approved by Customer that the Hosting Provider has retained for the purpose of providing connectivity for the Hosting Services in accordance with service level standards.
	Back Out Plan	Back Out Plan means a list of steps, and the roles or individuals responsible for performing such steps that are required to reverse Changes that had been applied to Customer's Production and Non-Production Environments.
	Base Configuration	Base Configuration means the standard amount of server, storage, networking, firewall, load balancing provided for Customer's Environments.
	Base Products	Base Products are unaltered software components, such as executable programs and compiled libraries.
	Batch Management Software	Batch Management Software means software to enable Hosting Provider to schedule, monitor, and manage batch workloads in Customer's Environment. An example of Batch Management Software is Concurrent Manager.
	Break-fix	Break-fix means a code change designed to restore, to its pre-Change state, the logic or functionality of a CEMLI that had been affected by a Change to an Environment.
	Business Intelligence Technology and Application Pro	Business Intelligence Technology and Applications Program means an Program identified by a Business Intelligence Application or a Business Intelligence Technology Program.
	Capacity Management	Capacity Management means the process of planning, analyzing, and sizing storage and transaction processing capability to enable the Production Environment to handle data processing demand.
	CEMLI	CEMLI is an acronym for any "configuration, extension, modification, localization, and integration," made to any Program.

	Certified Configuration	Certified Configuration means the combination of the configuration, instances, Programs, and the operating system, as provided by Hosting Provider, that is compliant with Hosting Provider standards and policies.
	Change	Change means a Hosting Provider- or Customer-initiated deployment of a specific addition, modification or removal, of a component, item, feature or function, to an Environment. Examples of Changes are the deployment of a Release into the Environment and a modification to the Environment configuration.
	Change Action Plan	Change Action Plan means a plan that identifies the steps, and the roles or individuals responsible for performing such steps that are required to complete a specific Change to an Environment.
	Change Management	Change Management means the management and deployment of Changes to an Environment.
	Change Request	Change Request means a request by Customer via Hosting Provider Change Management process for a Change to an Environment.
	Code Refresh	Code Refresh means the process of copying the full application code from a Source Environment to a Target Environment and making the required configuration Changes within the application tier of the Target Environment.
	Computer and Administration Services	Computer and Administration Services mean Application Management Services delivered by Hosting Provider deployment model.
	Concurrent Manager	Concurrent Manager is an example of Batch Management Software.
	Concurrent Peoplesoft Enterprise Users	Concurrent PeopleSoft Enterprise Users means the number of PeopleSoft Enterprise - Professional Application Users, PeopleSoft Enterprise CRM Self Service Application Users, PeopleSoft Enterprise Financials Self Service Application Users, PeopleSoft Enterprise Human Resources Self Service Application Users, PeopleSoft Enterprise Portal Self Service Application Users, and PeopleSoft Enterprise Learning Solutions Self Service Application Users simultaneously logged into the Environment.
	Configuration Migration	Configuration Migration means the process of copying application metadata and artifacts from a Source Environment to a Target Environment and making the required configuration Changes within the Target Environment.
	Contract Document	Contract Document means the contract signed by both Hosting Provider and Customer that is governed by the Agreement that outlines the Hosting Provider Programs and Services.
	Core Services	Core Services means Computer and Administration Services or Administration Services.
	CPE	CPE means Customer-provided network equipment.
	Critical Patch Updates	Critical Patch Updates means updates that are provided to Customer by Hosting Provider's Support Services organization as part of provider's technical support services and that are applied to the Environment as part of the Emergency Release Management process. Critical Patch Updates are designed to address significant security vulnerabilities and other issues that may relate to, or serve as prerequisites to, security issues, and may also include non-security fixes that are designed to address interdependency issues related to security patches.
	CSI	CSI means the Customer Support Identifier that is used by Customer to access and receive services from Hosting Provider Support and the Hosting Provider Service Desk.
	Custom Services	Custom Services mean services performed by Hosting Provider.
	Customer	Customer means the entity: State of Vermont.
	Customer Controlled Environments	Customer-Controlled Environments mean the environments identified in which Customer or its designee is authorized by Hosting Provider to use, apply Changes to, and maintain. Possible uses of Customer-Controlled Environments are development or testing.
	Customer Handling Instructions	Customer Handling Instructions means Customer-specific information in Hosting Provider's support system that is used by Hosting Provider personnel performing services for Customer.
	Customer Provided Network Equipement	Customer-Provided Network Equipment means network devices and circuits provided and managed by Customer that are installed in Hosting Provider's Data Center.
	Customer System Integrator	Customer System Integrator means entities given authority to act on behalf of the Customer in the areas of software development and configuration following the Hosting Providers change and configuration management process.

	Customers Data Center	Customer's Data Center means the Data Center retained and managed by Customer, or by a third party retained by Customer.
	Customers Help Desk	Customer's Help Desk means the point of contact provided by Customer for its End Users with respect to questions or issues that arise regarding the Hosting Provider Services and Environments.
	Data Center	Data Center means the physical location where the Environments for which Hosting Provider performs Hosting Provider Services reside.
	Data Center Security Policy	Data Center Security Policy means a document prepared and maintained by Hosting Provider that outlines access control requirements applicable to Hosting Provider's Data Center, including access requests, physical screening, on-site behavior and prohibited items.
	Database Refresh	Database Refresh means the process of copying a database from a Source Environment to a Target Environment and making the required configuration Changes within the database of the Target Environment.
	Decommission	Decommission means the process defined by Hosting Provider under which Customer's use of Hosting Provider Environments is ended and the Hosting Provider Services are terminated.
	Decommission Tape	Decommission Tape means the magnetic tapes provided by Hosting Provider as part of the Decommission of Computer and Administration Services that contain a copy of the production data from Customer's Production Environment.
	Dedicated	Means isolated physical and virtual infrastructure for purpose of completely segregating Customer environments from other Hosting Provider tenants. Including firewall, load balancer, switch, router, server, storage.
	Default-deny	Default-deny is a network-oriented approach to access control that implicitly denies the transmission of all network traffic but then specifically allows only required network traffic based on protocol, port, source, and destination.
	Demilitarized Zone	Demilitarized Zone means the "neutral zone" between the Internet and Hosting Provider's, or as applicable, a Customer's, private network.
	Demo and Demo Environment	Demo, and Demo Environment, means a Demonstration Environment.
	Demonstration Environment	Demonstration Environment means a type of Production Support Environment that is used for demonstration purposes.
	Dev and Dev Environment	Dev, and Dev Environment, means a Development Environment.
	Development Environment	Development Environment means a type of Non-Production Environment in which Customer or Customer Alternate performs development activities in support of Hosting Provider Services, such as the creation of customizations.
	Diagnostic Server	Diagnostic Server means a server enabled by Hosting Provider as part of Administration Services to remotely monitor the status and operation of Customer's Environment.
	Disaster	Disaster means an Unplanned Outage that causes a complete loss of access to and use of the Hosting Provider Programs in the Production Environment at the Primary Site for a period greater than 24 hours.
	Disaster Recovery	Disaster Recovery means services provided by Hosting Provider in accordance with the applicable Schedule to recover Production Environment data and to re-establish the Production Environment.
	Disaster Recovery Environment	Disaster Recovery Environment means the instance within the Secondary Site that mirrors Production in capacity, configuration in every way for the sole purpose of maintaining and operating Customers Production applications in the event of a disruption to the Hosting Providers services in Primary Site.
	Disaster Recovery Plan	Disaster Recovery Plan means a plan prepared and maintained by Hosting Provider that identifies tasks related to recovery and business continuity in the event of a Disaster.
	DLP or Data Loss Prevention	DLP or Data Loss Prevention means a system that is designed to detect potential data breach incidents in timely manner and prevent them by monitoring data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
	DMZ Server	DMZ Server for Hosting Provider Managed Applications means a public-facing application server or web server located in the Demilitarized Zone.
	DNS	DNS means the translation of a URL text address (e.g., state.vt.us) into a numeric Internet address (e.g., 200.213.11.6).
	DR	DR means Disaster Recovery.

	Duty Manager	Duty Manager means the Hosting Provider personnel identified by Hosting Provider as Customer's point of contact for escalating Service Requests within Hosting Provider.
	Embedded Software	Embedded Software is Third Party Software that is incorporated by Hosting Provider into certain Hosting Provider Programs.
	Emergency Release Management	Emergency Release Management means the process by which Critical Patch Updates are applied to Customer's Environment.
	End User	End User means an individual who is authorized by Customer to use the Hosting Provider Programs within the Environment.
	Enhanced Recovery Services	Enhanced Recovery Services means the Service under which Hosting Provider provides Disaster Recovery services – to meet Production RPO and RTO.
	Enterprise Governance	Enterprise Governance, Risk, and Compliance Program means an Hosting Provider Program identified by Hosting Provider as an Enterprise Governance, Risk, and Compliance Program.
	Entitlement	Entitlement means the base level of services that are included as part of Hosting Provider's standard Hosting Provider Services.
	Environment	Environment means the combination of Infrastructure and supporting software that is (i) configured for the Hosting Provider Programs operating on it and for specific uses as part of the Hosting Provider Services, and (ii) used by Hosting Provider to perform Hosting Provider Services. For Computer and Administration Services and Administration Services, the Environment consists of the Production Environment, any Production Support Environment(s) and any Non-Production Environment(s).
	Environment Plan	Environment Plan means a document prepared and maintained by Hosting Provider that identifies the environments used during implementation of the Hosting Provider Services and their respective purposes, such as development, CEMLI design and test, UAT, or staging purposes.
	Federal Environment	Federal Environment means a dedicated, caged Hosting Provider Environment at Hosting Provider's Data Center for United States federal government entity customers that purchase Computer and Administration Services and Hosting Provider's Federal Security Services.
	Federal Security Services	Federal Security Services means a Service Option applicable to Computer and Administration Services for United States federal government Customers, as described in the Federal Security Services Schedule.
	Full Refresh	Full Refresh means the process of copying of the database and full application code from a Source Environment to a Target Environment and making the required configuration Changes within the database and application tier of the Target Environment.
	Functional Service Desk	Functional Service Desk means services under which Hosting Provider Hosting Provider creates, receives, monitors, routes, and closes Functional Service Desk Service Requests.
	Functional Service Desk Service Request	Functional Service Desk Service Request means a request for assistance with Customer's Environment or any component thereof submitted to the Functional Service Desk.
	Go-Live	Go-Live means Production Go-Live.
	Hosting Provider	Hosting Provider means the Hosting Provider line of business that delivers the Hosting Provider Services.
	Hosting Provider Application List	Hosting Provider Application List is a document that lists all application programs covered by Hosting Provider services.
	Hosting Provider Continuous Connection Network	Hosting Provider Continuous Connection Network means a dedicated network designed to support Network Connectivity between Hosting Provider and Customer's Environment, and that uses the following elements: a firewall, VPN, intrusion detection, authentication, reporting, and DNS.
	Hosting Provider Controlled Environments	Hosting Provider-Controlled Environments are those environments in which Hosting Provider has sole control to make Changes.
	Hosting Provider Controlled Infrastructure	Hosting Provider-Controlled Infrastructure means Infrastructure used for Administration Services that is managed and maintained solely by Hosting Provider.

	Hosting Provider Customer Portal	Hosting Provider Customer Portal means the Customer-specific Internet based portal provided by Hosting Provider to Customer as part of the Hosting Provider Services by which Customer may view performance reports generated by Hosting Provider and the status of Service Requests.
	Hosting Provider Data Center	Hosting Provider Data Center means Hosting Provider's Data Center. Hosting Provider's Data Center means the Data Center(s) retained and managed by Hosting Provider, or by a third party retained by Hosting Provider, at which Hosting Provider delivers Hosting Provider Hosting Provider Services.
	Hosting Provider Data Center Badge Access	Hosting Provider Data Center Badge Access Form means an Hosting Provider form that must be completed by a person seeking to visit Hosting Provider's Data Center. Once completed by the visitor, the form is forwarded within Hosting Provider for review and approval purposes, and is retained by Hosting Provider in accordance with Hosting Provider policy.
	Hosting Provider Internal Support Network	Hosting Provider Internal Support Network is comprised of a firewall, VPN, intrusion detection, authentication, reporting, and DNS. This isolated network is the standard Network Connectivity option for Hosting Provider personnel to connect to the Environment.
	Hosting Provider Product Issue	Hosting Provider Product Issue means an Incident associated with the functioning of Hosting Provider Program(s) (including program errors) but is not caused by Hosting Provider's performance of Hosting Provider Services.
	Hosting Provider Program	Hosting Provider Program means the Hosting Provider software product licensed to Customer separately and for which Hosting Provider Hosting Provider performs Hosting Provider Services. Hosting Provider Programs shall be deemed to mean all the Hosting Provider Programs identified for which Hosting Provider is providing Hosting Provider Services. Hosting Provider Programs may include Hosting E-Business Suite Programs, PeopleSoft Enterprise Programs, Siebel CRM Programs, Hosting Provider Technology Programs, Hosting Provider Hyperion Programs, Business Intelligence Technology and Applications Programs, Retail Programs, Agile Product Lifecycle Management Programs, Enterprise Governance, Risk, and Compliance Programs, User Productivity Kit Programs. The term Hosting Provider Program includes any Embedded Software within the applicable Hosting Provider Program.
	Hosting Provider Project Plan	Hosting Provider Project Plan means the document prepared by Hosting Provider that outlines the tasks to be performed by Hosting Provider, including anticipated start and end dates, for Transition Advisory Services.
	Hosting Provider Service Desk	Hosting Provider Service Desk means a team of resources provided by Hosting Provider Hosting Provider as part of Hosting Provider Services, under which Hosting Provider Hosting Provider creates, receives, monitors, routes, and closes Service Requests or Incidents, as described in the applicable Schedule.
	Hosting Provider Support	Hosting Provider Support means the Hosting Provider technical support organization (Hosting Provider Support Services) that provides product-related technical support services for Hosting Provider Programs.
	Hosting Provider Technology Program	Hosting Provider Technology Program means an Hosting Provider Program identified by Hosting Provider as a Technology Program. Hosting Provider performs Hosting Provider Services under an applicable agreement.
	HPCCN	HPCCN means Hosting Provider Continuous Connection Network.
	HPCP	HPCP means Hosting Provider Hosting Provider Customer Portal.
	HPISN	Means Hosting Provider Internal Support Network
	IDS or Intrusion Detection System	IDS or Intrusion Detection System means a system that monitors Customer's Environment for security violations such as attack signatures, anomalous ports, and anomalous protocols being accessed.
	Implementer	Implementer means a Third Party Vendor or Software Integrator retained by Customer to provide implementation services to Customer in support of Hosting Provider Services. For the purpose of this definition, an Implementer may be Hosting Provider's Consulting line of business.
	Incident	Incident means any event experienced by Customer in its use of the Hosting Provider Services for which a Service Request has been submitted, that is not consistent with the standard, documented operation of the Hosting Provider Services, and which causes, or may cause, a Service Interruption.

	Individual Patch	Individual Patch means a software fix, created by Hosting Provider, to an Hosting Provider Program and provided between patch set Releases. Individual Patches are designed to address specific software errors or vulnerabilities but not otherwise intended to change the functionality of programs.
	Information Security Incident Response Lead	Information Security Incident Response Lead means the Hosting Provider employee assigned by Hosting Provider to lead Hosting Provider's response to Severity 1 and Severity 2 information security Incidents.
	Information Security Incident Response Plan	Information Security Incident Response Plan (ISIRP) means a document prepared by Hosting Provider that details activities that are to be performed in the event of an information security Incident related to the applicable Environment and Hosting Provider Services. Hosting Provider periodically updates the ISIRP document to reflect current information security Incident response planning.
	Information Security Incident Response Team	Information Security Incident Response Team means the Hosting Provider team that is designated by Hosting Provider to prepare for, and respond to, information security Incidents.
	Information Security Manager	Information Security Manager means an Hosting Provider employee designated by Hosting Provider to act as a liaison regarding security issues that affects the applicable Hosting Provider line of business. Each Hosting Provider line of business unit may have an Information Security Manager.
	Infrastructure	Infrastructure means the combination of Hosting Provider's Data Center, hardware, servers, virtualization, operating system, storage, and networking equipment, used for the delivery of Hosting Provider Services.
	Infrastructure Requirements	Infrastructure Requirements means information provided by Customer in the Infrastructure Requirements Document regarding the Infrastructure for the Hosting Provider Services, such as capacity and usage information.
	Infrastructure Requirements Document	Infrastructure Requirements Document means the document required by Hosting Provider in which Customer specifies its Infrastructure Requirements.
	Internet Protocol Security	Internet Protocol Security means a security framework based on open standards and designed to protect communications over Internet Protocol networks through the use of cryptography.
	Ipsec	IPsec means Internet Protocol Security.
	ISIRL	ISIRL is the Information Security Incident Response Leader.
	ISIRP	ISIRP means Information Security Incident Response Plan.
	ISIRT	ISIRT means Information Security Incident Response Team.
	ISM	ISM means an Information Security Manager.
	Least Privilege	Least Privilege means a system-oriented approach to access control under which user permissions and system functionality are specifically evaluated and access is restricted to the resources required for users or systems to perform their respective duties.
	Maintenance Code Release	Maintenance Code Release means any Release designed to address the manner in which Hosting Provider Programs process data or operate, and neither contains new functionality nor changes the results of processing data. Examples of Maintenance Code Releases are Individual Patches, tool updates, tax updates, bug fixes, and maintenance packs. The term Maintenance Code Release specifically excludes any Service Pack or Upgrade.
	Maintenance Window	Maintenance Window means, depending on the context, a Weekly Maintenance Window, a Semiannual Maintenance Window, or any other period of time scheduled by Hosting Provider for a Planned Outage within which Hosting Provider may perform maintenance activities on Infrastructure.
	Major Maintenance Window	Major Maintenance Window means the agreed to time when Hosting Provider can perform system maintenance/configuration changes on Production Environment that will reduce or make the Production Environment unavailable.
	Major Release	Major Release means an Upgrade that is designated as follows: (i) for all Hosting Provider Programs by the identifying first number of the Upgrade (e.g., change from Application 9.x to Application 10.x), and (ii) for PeopleSoft Enterprise Programs, by the identifying first number of the Upgrade after the decimal place (e.g., change from version 9.1 to 9.2).
	Major Upgrade	Major Upgrade means a Major Release.

	Management Link	Management Link means the type of Network Connectivity used for Administrations Services.
	Migration Readiness Assessment	Migration Readiness Assessment means a document that contains Hosting Provider's assessment of Customer's Infrastructure and that is used for creating a Production Environment that conforms to Hosting Provider's Certified Configuration.
	Minor CEMLI Enhancement Request	Minor CEMLI Enhancement Request means a request by Customer, via Hosting Provider's Change Management process, for Hosting Provider Hosting Provider to enhance a CEMLI to an Hosting Provider Program within Customer's Environment, where such enhancement is designed to improve the functionality of the CEMLI and does not require Hosting Provider more than 40 person hours to perform. A "person hour" is one hour of work performed by one Hosting Provider resource.
	Minor Maintenance Window	Minor Maintenance Window means the agreed to time when Hosting Provider can perform system maintenance/configuration changes on Production Environment that will have no effect on Production Environment availability.
	Minor Release	Minor Release means an Upgrade that contains new functionality and that is upwardly compatible to an earlier Release of the applicable Hosting Provider Program.
	My Hosting Provider Support	My Hosting Provider Support means Hosting Provider's web-based customer support system under which Hosting Provider provides technical support for Hosting Provider Programs and by which Customer may submit Service Requests. Customer obtains the use of My Hosting Provider Support by purchasing technical support services from Hosting Provider.
	Non-Production Environment	Non-Production Environment means an instance that is specifically configured for Customer's use (or, as applicable, Customer's Implementer's use) of the Hosting Provider Programs for non-production activities that relate to the Hosting Provider Services, such as development, training, data conversion, and CEMLI maintenance.
	North American Data Center	North America Data Center means the U.S. Data Center.
	Optional Third Party Software	Optional Third Party Software means any Third Party Software not supplied by Hosting Provider.
	OS	OS means operating system.
	Outage	Outage means a complete loss of access to and use of the Production Environment, the Production Support Environment, the Non-Production Environment, or the Pre-Production Environment. An Outage may be a Planned Outage or an Unplanned Outage.
	Overall Program Plan	Overall Program Plan means a project plan prepared by Hosting Provider that outlines the necessary tasks, task performance schedules, and the roles or individuals required to perform such tasks, for a transition.
	Partial Refresh	Partial Refresh means the process of copying a database and/or a portion of application code from a Source Environment to a Target Environment and making the required configuration Changes within the database and application tier of the Target Environment.
	Password Manager Utility	Password Manager Utility means an Hosting Provider-proprietary Tool used by Hosting Provider to manage passwords and provide controlled-access to database and application passwords to those End Users who have named Linux/Windows operating system accounts.
	Peoplesoft Applications	PeopleSoft Enterprise CRM, Enterprise Financials, Human Resources, Portal, Performance Management, Learning Solutions
	Performance Management	Performance Management means a subset of Hosting Provider Services under which Hosting Provider manages the speed of transaction response of the Hosting Provider Programs, and batch job execution in the Production Environment.
	Periodic Maintenance Plan	Periodic Maintenance Plan means a written plan prepared and maintained by Hosting Provider that generally describes the schedule for the application of Changes, new Releases, and Upgrades, to the Production Environment.
	Planned Outage	Planned Outage means an Outage scheduled by Hosting Provider during which Hosting Provider performs system maintenance and other activities for the Environment and the Hosting Provider Services.
	PMP	PMP means Periodic Maintenance Plan.

	Point Release	Point Release means a Minor Release.
	Post Production Go-Live	Post Production Go-Live means the period following the Production Go-Live of the Production Environment.
	Pre-Production Environment	Pre-Production Environment means the instance within the Environment that mirrors Production in capacity, configuration in every way for the sole purpose of applying and testing all changes, hot fixes, patches, code release and/or upgrades before releasing changes to Production.
	Primary Site	Primary Site means the Data Center at which Customer's Environment is located and at which Hosting Provider delivers Hosting Provider Services. The Environment and the delivery of Hosting Provider Services may be relocated to a Secondary Site in the event of a Disaster.
	Priority Level	Priority Level means the classification used in conjunction with Severity Level to identify the priority of a Service Request with respect to the Hosting Provider Services.
	Problem	Problem means (i) the collection of multiple recurring Incidents that exhibit common symptoms and that originate from a single, common cause, and for which the cause is unknown, or (ii) a single Incident that results from a single error and that has an on-going significant impact on the Hosting Provider Services (such as an Unplanned Outage), and for which the cause is unknown.
	Problem Management	Problem Management means a subset of Hosting Provider Services under which Hosting Provider manages Problems within Customer's Environment.
	Production Assessment	Production Assessment means a document that is prepared by Hosting Provider prior to Production Go-Live and that contains Hosting Provider's assessment of the compliance of Customers' Environment with Hosting Provider Hosting Provider standards.
	Production Environment	Production Environment means the instance within the Environment that is specifically set up and configured to support Customer's use of the Hosting Provider Programs, and used by Customer, for production operations. The Production Environment consists of the collection of database servers, application ("mid-tier") servers, and other servers comprising Customer's transactional production system.
	Production Go-Live	Production Go-Live means the date on which Customer first commences use of the Production Environment for production operations (i.e., to process live data).
	Production Ready Status	Production Ready Status means a designation given by Hosting Provider to Customer indicating that Customer may commence use of a Production Environment for production operations.
	Production Support Environments	Production Support Environment means the TEST and DEMO Environments that are specifically set up and configured in a manner that closely resembles the Production Environment, and that are used, as applicable, to troubleshoot and facilitate Incident resolution, to test changes prior to promotion of such changes to the Production Environment and for demonstration purposes.
	Program Responsibilities	Program Responsibilities means the functionality that a User may use within the Hosting Provider Programs.
	Program-Specific Application Management	Program-Specific Application Management Services means the Application Management Services specifically applicable to a certain set of Hosting Provider Programs.
	Program-Specific Standards	Program-Specific Standards means the Standards Schedule specifically applicable to a certain set of Hosting Provider Programs.
	Provosioning Release Plan	Provisioning Release Plan means a document or set of documents prepared by Hosting Provider that describes the installation and configuration of hardware and software required for the Hosting Provider Environment.
	RCA	RCA means Root Cause Analysis.
	Recovery Point Objective or RPO	Recovery Point Objective or RPO means Hosting Provider's objective for the potential maximum time period of data loss, calculated from the onset of a Disaster.
	Recovery Time Objective or RTO	Recovery Time Objective or RTO means Hosting Provider's objective for the potential maximum period of time between the declaration of a Disaster and the point at which Customer can resume production operations in the Production Environment.

	Refresh	Refresh means the process of copying a Customer's database files, application files, and/or the application metadata and artifacts from a Source Environment to a Target Environment and updating related configurations within the Environment.
	Release	Release means a software change or set of software changes, to Hosting Provider Programs, that is provided to Customer by Hosting Provider's Support Services organization as part of Hosting Provider's technical support services. The term Release includes Upgrades and Maintenance Code Releases.
	Release Management	Release Management means a subset of Hosting Provider Services under which Hosting Provider manages the deployment of Releases into Customer's Environment.
	Release Plan	Release Plan means a document that details the planning, testing, and executing of proposed Releases. The Release Plan includes a Back Out Plan.
	Request	Request for Change means Change Request.
	Required Software	Required Software means Third Party Software for which Hosting Provider requires Customer to separately purchase a license and technical support in connection with Hosting Provider Services for certain Hosting Provider Programs, and for which Hosting Provider expressly performs Hosting Provider Services.
	Restore	Restore means the process of copying a database and/or full application code from a disk or tape backup to the Environment from which the copy was made.
	RFC	RFC means Request for Change.
	Root Cause Analysis	Root Cause Analysis means a process by which Hosting Provider seeks to determine the root cause of a Problem and/or an Incident, identify details of any work-around including reasons for the work-around as applicable, and the history of the Problem or Incident.
	Sandbox or Sandbox Environment	Sandbox, or Sandbox Environment, means a type of Production Support Environment that is used by Customer for the purposes of prototyping, alternative analysis, proof of concept. This environment is not in the development life cycle.
	Secondary Site	Secondary Site means the Data Center other than the Primary Site to which the Environment and delivery of Hosting Provider Services is relocated in the event of a Disaster.
	Siebel Applications	Siebel CRM Communications, Media and Energy, Siebel CRM Life Sciences, Siebel CRM Manufacturing and Distribution, Siebel CRM Financial Services, Siebel CRM Public Sector, Siebel CRM Horizontal Applications
	Siebel Applications	Siebel CRM Communications, Media and Energy, Siebel CRM Life Sciences, Siebel CRM Manufacturing and Distribution, Siebel CRM Financial Services, Siebel CRM Public Sector, Siebel CRM Horizontal Applications
	Semiannual Maintenance Window	Semiannual Maintenance Window means the period of time, to occur approximately every six months, during which Hosting Provider may schedule Planned Outages to perform maintenance activities on Infrastructure. The maintenance activities typically performed by Hosting Provider during a Semiannual Maintenance Window involve components of the Infrastructure that are used to deliver Hosting Provider Services specifically to Customer.
	Server	Server means a computing platform with defined processing power, memory capacity, and operating system. The Server may be implemented as a virtual or shared allocation from one or more physical computing platform(s).
	Server for Customer Managed Applications	Server for Customer Managed Applications means a Service Option under which Hosting Provider initializes and installs operating system software on an Hosting Provider-provisioned server to enable Customer to access, manage, and monitor such server.
	Server for Hosting Provider Managed Applications	Server for Hosting Provider Managed Applications means the Service Option for Computer and Administration Services under which a server is added by Hosting Provider to Customer's Environment to support additional environments.
	Service continuity Management	Service Continuity Management means a subset of Hosting Provider Services under which Hosting Provider continues to deliver Computer and Administration Services for the Production Environment following a Disaster.

	Service Interruption	Service Interruption means a material reduction of the functionality and responsiveness of a component of the Production Environment, a Production Support Environment, or a Non-Production Environment, such that Customer's ability to use the Hosting Provider Services to process one or more of Customer's key business transactions is significantly impacted.
	Service Pack	Service Pack means a Minor Release.
	Service Request	Service Request means a request for assistance with the Environment or any component thereof submitted to My Hosting Provider Support or the Hosting Provider Service Desk.
	Service-Specific Application Management	Service-Specific Application Management Services Schedule means Program-Specific Application Management Services Schedule.
	Service-Specific Standards	Service-Specific Standards means Program-Specific Standards.
	Severity Level	Severity Level means the level of criticality assigned to a Service Request based on defined criteria.
	Siebel CRM Program	Siebel CRM Program means an Hosting Provider Program identified by Hosting Provider as an Hosting Provider Siebel CRM Program. Hosting Provider performs Hosting Provider Siebel Programs.
	Site	Site means a website for which Hosting Provider Services for all Programs.
	Site Go-Live	Site Go-Live means the date on which a Site first becomes available to the general public and transactions can be processed on the Site.
	SOP	SOP means Standard Operating Procedures.
	Source Environment	Source Environment means a Production Environment, Production Support Environment or Non-Production Environment from which data for a Refresh is obtained.
	SR	SR means a Service Request.
	SSL	SSL means "secure sockets layer," a commonly used protocol for managing the security of a data transmission on the Internet. SSL uses a public-and-private key encryption system, which also includes the use of a digital certificate.
	Staging or Staging Environment	Means Pre-Production Environment.
	Standard Operating Procedures	Standard Operating Procedures mean Hosting Provider's set of security-focused processes that set forth the standard procedures, activities and tasks performed by Hosting Provider resources while delivering Hosting Provider Services to Hosting Provider customers.
	Standy Envrionment	Standby Environment means an Environment located at the Secondary Site that closely resembles the capacity and performance capabilities of the Production Environment at the Primary Site, and that may be used for production operations in the event of a Disaster.
	Storage Unit	Storage Unit means a unit of usable Gigabytes of disk storage.
	Super User	Super User means an End User that Customer has assigned to assist other End Users in the use of Hosting Provider Services. Super Users serve as the liaison between End Users, Customer's Help Desk, and the Hosting Provider Service Desk.
	Supplemental Services	Supplemental Services mean Service Options.
	Supported CEMLIs	Supported CEMLIs mean CEMLIs that were reviewed and approved by Hosting Provider as part of the Production Assessment process and for which Hosting Provider provides Hosting Provider Services in the Production Environment.
	Systems Administrator	System Administrator means an Hosting Provider resource assigned by Hosting Provider to perform tasks to maintain the Environment as part of the Hosting Provider Services.
	Target Environment	Target Environment means the Production Environment, Production Support Environment or Non-Production Environment to which data for a Refresh will be applied.
	Technology stack	Technology Stack means any database, operating system and middleware used in an Environment.
	Test or Test Environment	Test, or Test Environment, means a type of Production Support Environment that is used by Hosting Provider for testing and validating Changes prior to promotion to the Production Environment as well as for recreating events and duplicating issues occurring in the Production Environment for the purposes of troubleshooting and facilitating Incident resolution.

	Third Part Software	Third Party Software means any software from a Third Party Software Vendor, which is not provided by Hosting Provider as part of the Hosting Provider Services, and any software developed or provided by Customer.
	Third Party Vendor	Third Party Vendor means a provider, other than Hosting Provider, of products or services.
	Tools	Tools mean software scripts provided and used by Hosting Provider in the Environment for the delivery of Hosting Provider Services (e.g., to perform environment clones, password changes, service monitoring, and file system maintenance).
	Training or Training Environment	Training, or Training Environment, means a type of Production Support Environment that is used by Customer for the purposes of training.
	Transaction Link	Transaction Link means the type of Network Connectivity used for Computer and Administration Services.
	Transition	Transition means the activities completed and modifications made to a Customer's system and/or to an Hosting Provider Environment as part of Transition Advisory Services.
	Transition Advisory Services	Transition Advisory Services means a service performed by Hosting Provider to convert a Customer's system to an Hosting Provider Environment or to make significant Changes (such as an Upgrade) to an existing Hosting Provider Environment.
	U.S.Data Center	U.S. Data Center means Hosting Provider's Data Center(s) located in the United States.
	UAT	UAT means User Acceptance Testing.
	UAT Environment	UAT Environment, means a type of Production Support Environment that is used by Customer for testing User Acceptance and validating Changes prior to promotion to the Production Environment.
	United States Data Center	United States Data Center means U.S. Data Center
	Unplanned Outage	Unplanned Outage means an Outage that was not scheduled by Hosting Provider or Customer and is caused by an Incident or Problem.
	Upgrade	Upgrade means a new Release of an Hosting Provider Program that contains new functionality and/or under which the results of how such program processes data differs as compared to an earlier Release of such program.
	User	User means an End User.
	User Acceptance Testing	User Acceptance Testing means a formal testing process that is part of the Change Management Process conducted by Customer of a specified Change to the Environment for the purpose of determining whether such Change meets identified acceptance criteria.
	VPN	VPN means Virtual Private Network.
	WAN	WAN means Wide Area Network.
	Weekly Maintenance Window	Weekly Maintenance Window means the period of time, to occur once per week, during which Hosting Provider may schedule Planned Outages to perform maintenance activities on Infrastructure. The maintenance activities typically performed by Hosting Provider during a Weekly Maintenance Window involve components of the Infrastructure that are used to deliver Hosting Provider Services to Hosting Provider's customers generally, including to Customer.
	Windows Software Update Service	Windows Software Update Service means a Microsoft service provided to Hosting Provider under which Microsoft delivers current security updates to Hosting Provider-owned Windows-based computers.
	WSUS	WSUS means Windows Software Update Service.
		Hosting Provider Services mean, collectively and as applicable, the Computer and Administration Services, Administration Services, and all other services provided by Hosting Provider Hosting Provider, including associated Service Options, which are ordered under and identified in the Ordering Document.

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Data Center (DC) General

Base	Level	Sub	Req ID	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
DC	1	1	DC.1.1	Data Center		Data center design and operations will be Tier 3 equivalent or higher per TIA 942 standards. See H1B TIA 942	No	We are not Tier 3 in all areas, but have amny tier 3 characteristics.	
DC	1	2	DC.1.2	Data Center		Data center facilities will be located in the continental united states.	Yes		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Data Center (DC) TIA 942 Standards

Base	Level	Sub	Req ID	Focus	Specifics	Tier Requirements	Tier 1	Tier 2	Tier 3	Tier 4	Tier Rating	Notes	Evidence
TIA	1	1	TIA.1.1	Data Center (Architectural)	Location	Proximity to flood hazard area as mapped on a federal Flood Hazard Boundary or Flood Insurance Rate Map	no requirement	not within flood hazard area	Not within 100-year flood hazard area and greater than 91 m / 100 yards from 50-year flood hazard area	Greater than 91 m / 100 yards from 100-year flood hazard area	T3		
TIA	1	2	TIA.1.2	Data Center (Architectural)	Location	Proximity to coastal or inland waterways	no requirement	no requirement	Greater than 91 m/ 100 yards	Greater than 0.8 km / 1/2 mile	T4		
TIA	1	3	TIA.1.3	Data Center (Architectural)	Location	Proximity to major traffic arteries	no requirement	no requirement	Greater than 91 m / 100 yards	Greater than 0.8 km / 1/2 mile	T3		
TIA	1	4	TIA.1.4	Data Center (Architectural)	Location	Proximity to airports	no requirement	no requirement	Greater than 1.6 km / 1 mile and less than 30 miles	Greater than 8 km / 5 miles and less than 30 miles	T4		
TIA	1	5	TIA.1.5	Data Center (Architectural)	Location	Proximity to major metropolitan area	no requirement	no requirement	Less than 48 km / 30 miles	Less than 16 km / 10 miles	T4		
TIA	1	6	TIA.1.6	Data Center (Architectural)	Parking	Separate visitor and employee parking areas	no requirement	no requirement	yes (physically separated by separated entries)	yes (physically separated by fence or wall with separated entries)	T2		
TIA	1	7	TIA.1.7	Data Center (Architectural)	Parking	Separate from loading docks	no requirement	no requirement	yes (physically separated by separated entries)	yes (physically separated by fence or wall with separated entries)	T4		
TIA	1	8	TIA.1.8	Data Center (Architectural)	Parking	Proximity of visitor parking to data center perimeter building walls	no requirement	no requirement	9.1 m / 30 ft minimum separation with physical barriers to prevent vehicles from driving closer	18.3 m / 60 ft minimum separation with physical barriers to prevent vehicles from driving closer	T2		
TIA	1	9	TIA.1.9	Data Center (Architectural)	Multi-tenant occupancy within building	***Multi-tenant occupancy within building***	no restriction	Allowed only if occupancies are non-hazardous	Allowed if all tenants are data centers or telecommunications companies	Allowed if all tenants are data centers or telecommunications companies	N/A	CGI is Sole tenant	
TIA	1	10	TIA.1.10	Data Center (Architectural)	Building construction	Type of construction	no restriction	no restriction	Type IIA, IIIA, or VA	Type IA or IB	T3		
TIA	1	11	TIA.1.11	Data Center (Architectural)	Building construction	Fire resistive requirements	no requirement	no requirement	no requirement	no requirement	T4		
TIA	1	12	TIA.1.12	Data Center (Architectural)	Building construction	Exterior bearing walls	Code allowable	Code allowable	1 Hour minimum	4 Hours minimum	T3		
TIA	1	13	TIA.1.13	Data Center (Architectural)	Building construction	Interior bearing walls	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	14	TIA.1.14	Data Center (Architectural)	Building construction	Exterior nonbearing walls	Code allowable	Code allowable	1 Hour minimum	4 Hours minimum	T3		
TIA	1	15	TIA.1.15	Data Center (Architectural)	Building construction	Structural frame	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	16	TIA.1.16	Data Center (Architectural)	Building construction	Interior non-computer room partition walls	Code allowable	Code allowable	1 Hour minimum	1 Hour minimum	T4		
TIA	1	17	TIA.1.17	Data Center (Architectural)	Building construction	Interior computer room partition walls	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	18	TIA.1.18	Data Center (Architectural)	Building construction	Shaft enclosures	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	N/A		
TIA	1	19	TIA.1.19	Data Center (Architectural)	Building construction	Floors and floor-ceilings	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	20	TIA.1.20	Data Center (Architectural)	Building construction	Roofs and roof-ceilings	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T3		
TIA	1	21	TIA.1.21	Data Center (Architectural)	Building construction	Meet requirements of NFPA 75	No requirements	yes	yes	yes		We believe "yes" but we are not sure.	
TIA	1	22	TIA.1.22	Data Center (Architectural)	Building Components	Vapor barriers for walls and ceiling of computer room	no requirement	yes for walls, no requirement for ceiling	yes	yes	T1	Not required for AZ climate	
TIA	1	23	TIA.1.23	Data Center (Architectural)	Building Components	Building entrances with security checkpoints	no requirement	no requirement	yes (primary building entrance manned)	yes (primary building entrance manned)	T4		
TIA	1	24	TIA.1.24	Data Center (Architectural)	Building Components	Access floor panel construction (when provided)	no requirement	no requirement	computer grade all steel	computer grade all steel or computer grade steel with concrete filled	T4		
TIA	1	25	TIA.1.25	Data Center (Architectural)	Building Components	Understructure (when access floor is provided)	no requirement	no requirement	bolted stringer	bolted stringer with 1.2 m x 1.2 m (4 ft x 4 ft) basket weave pattern	T4		
TIA	1	26	TIA.1.26	Data Center (Architectural)	Building Components	Ceilings within computer room areas (when provided)	no requirement	no requirement	no requirement	no requirement	T4		
TIA	1	27	TIA.1.27	Data Center (Architectural)	Building Components	Ceiling Construction	no requirement	no requirement	If provided, suspended with clean room class 10M-100M perforated tile	Suspended with clean room class 100 non-perforated vinyl coated gypsum board tiles tile	T3		

TIA	1	28	TIA.1.28	Data Center (Architectural)	Building Components	Ceiling Height (above raised access floor if provided)	2.6 m (8.5 ft) minimum	2.7 m (9.0 ft) minimum	3 m (10 ft) minimum (not less than 460 mm (18 in) above tallest piece of equipment	3 m (10 ft) minimum (not less than 600 mm/24 in above tallest piece of equipment)	T4		
TIA	1	29	TIA.1.29	Data Center (Architectural)	Roofing	Class	no restrictions	Class A	Class A	Class A	T4	reflective membrane is highly fire resistive	
TIA	1	30	TIA.1.30	Data Center (Architectural)	Roofing	Type	no restrictions	no restrictions	non-redundant with non-combustible deck (no mechanically attached systems)	double redundant with concrete deck (no mechanically attached systems)	T2		
TIA	1	31	TIA.1.31	Data Center (Architectural)	Roofing	Wind uplift resistance	Minimum Code requirements	FM I-90	FM I-90 minimum	FM I-120 minimum	T4		
TIA	1	32	TIA.1.32	Data Center (Architectural)	Roofing	Roof Slope	Minimum Code requirements	Minimum Code requirements	1:48 (1/4 in per foot) minimum	1:24 (1/2 in per foot) minimum	T3		
TIA	1	33	TIA.1.33	Data Center (Architectural)	Doors and Windows	F Fire rating	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 3/4 hour at computer room)	Minimum Code requirements (not less than 1 1/2 hour at computer room)	T4		
TIA	1	34	TIA.1.34	Data Center (Architectural)	Doors and Windows	Door size	Minimum Code requirements and not less than 1 m (3 ft) wide and 2.13 m (7 ft in) high	Minimum Code requirements and not less than 1 m (3 ft) wide and 2.13 m (7 ft) high	Minimum Code requirements (not less than 1 m (3 ft) wide into computer, electrical, & mechanical rooms) and not less than 2.13 m (7 ft) high	Minimum Code requirements (not less than 1.2 m (4 ft) wide into computer, electrical, & mechanical rooms) and not less than 2.13 m (7 ft) high	T3		
TIA	1	35	TIA.1.35	Data Center (Architectural)	Doors and Windows	Windows on perimeter of computer room	Allowed with minimum code required fire rating	Allowed with minimum code required fire rating	interior windows allowed with minimum 1-hour fire rating, no exterior windows allowed	interior windows allowed with minimum 1-hour fire rating, no exterior windows allowed	T4		
TIA	1	36	TIA.1.36	Data Center (Architectural)	Entry Lobby	Physically separate from other areas of data center	no requirement	yes	yes	yes	T4		
TIA	1	37	TIA.1.37	Data Center (Architectural)	Entry Lobby	Fire separation from other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)			
TIA	1	38	TIA.1.38	Data Center (Architectural)	Entry Lobby	Security counter	no requirement	no requirement	yes	yes (physically separated)	T4		
TIA	1	39	TIA.1.39	Data Center (Architectural)	Entry Lobby	Single person interlock, portal or other hardware designed to prevent piggybacking or pass back	no requirement	no requirement	yes	yes	T2	security manned 24x7x365, anti passback enabled	
TIA	1	40	TIA.1.40	Data Center (Architectural)	Administrative Offices	Physically separate from other areas of data center	no requirement	yes	yes	yes	T4		
TIA	1	41	TIA.1.41	Data Center (Architectural)	Administrative Offices	Fire separation from other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)	T4		
TIA	1	42	TIA.1.42	Data Center (Architectural)	Security Office	Physically separate from other areas of data center	no requirement	no requirement	yes	yes	T4		
TIA	1	43	TIA.1.43	Data Center (Architectural)	Security Office	Fire separation from other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)	T4		
TIA	1	44	TIA.1.44	Data Center (Architectural)	Security Office	180-degree peepholes on security equipment and monitoring rooms	No requirement	Yes	Yes	yes	T4		
TIA	1	45	TIA.1.45	Data Center (Architectural)	Security Office	Dedicated and harden security equipment and monitoring rooms	No requirement	Recommended	Recommended	Recommended	T4		
TIA	1	46	TIA.1.46	Data Center (Architectural)	Security Office	Dedicated security room for security equipment and monitoring	No requirement	Yes	Yes, with 16 mm (5/8 in) plywood lined walls and solid core door	Yes, with 16 mm (5/8 in) plywood lined walls and solid core door	T4		
TIA	1	47	TIA.1.47	Data Center (Architectural)	Security Office	Operations Center Physically separate from other areas of data center	no requirement	no requirement	yes	yes	T4		
TIA	1	48	TIA.1.48	Data Center (Architectural)	Security Office	Fire separation from other non-computer room areas of data center	no requirement	no requirement	1 hour	2 hour	T4		
TIA	1	49	TIA.1.49	Data Center (Architectural)	Security Office	Proximity to computer room	no requirement	no requirement	indirectly accessible (maximum of 1 adjoining room)	directly accessible	T3		
TIA	1	50	TIA.1.50	Data Center (Architectural)	Restroom and break room	Proximity to computer room and support areas	no requirement	no requirement	If immediately adjacent, provided with leak prevention barrier	Not immediately adjacent and provided with leak prevention barrier	T4		
TIA	1	51	TIA.1.51	Data Center (Architectural)	Restroom and break room	Fire separation from computer room and support areas	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)	T4		
TIA	1	52	TIA.1.52	Data Center (Architectural)	UPS and Battery Rooms	Aisle widths for maintenance, repair, or equipment removal	no requirement	no requirement	Minimum Code requirements (not less than 1 m (3 ft) clear)	Minimum Code requirements (not less than 1.2 m (4 ft) clear)	T4		

TIA	1	53	TIA.1.53	Data Center (Architectural)	UPS and Battery Rooms	Proximity to computer room	no requirement	no requirement	Immediately adjacent	Immediately adjacent	T4		
TIA	1	54	TIA.1.54	Data Center (Architectural)	UPS and Battery Rooms	Fire separation from computer room and other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)	T4		
TIA	1	55	TIA.1.55	Data Center (Architectural)	Required Exit Corridors	Fire separation from computer room and support areas	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)	T4		
TIA	1	56	TIA.1.56	Data Center (Architectural)	Required Exit Corridors	Width	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements and not less than 1.2 m (4 ft) clear	Minimum Code requirements and not less than 1.5 m (5 ft) clear)	T4		
TIA	1	57	TIA.1.57	Data Center (Architectural)	Shipping and receiving areas	Shipping and receiving area Physically separate from other areas of data center	No shipping and receiving area provided	No	yes	yes	T4		
TIA	1	58	TIA.1.58	Data Center (Architectural)	Shipping and receiving areas	Fire separation from other areas of data center	Minimum code requirements if shipping and receiving area present	Minimum code requirement	1 hour	2 hour	T4		
TIA	1	59	TIA.1.59	Data Center (Architectural)	Shipping and receiving areas	Physical protection of walls exposed to lifting equipment traffic	no requirement	no requirement	yes (minimum 19mm (3/4 in) plywood wainscot)	yes (steel bollards or similar protection)	T4		
TIA	1	60	TIA.1.60	Data Center (Architectural)	Shipping and receiving areas	Number of loading docks	no requirement	1 per 2500 sq m / 25,000 sq ft of Computer room	1 per 2500 sq m / 25,000 sq ft of Computer room (2 minimum)	1 per 2500 sq m / 25,000 sq ft of Computer room (2 minimum)	T4		
TIA	1	61	TIA.1.61	Data Center (Architectural)	Generator and fuel storage areas	Proximity to computer room and support areas	no requirement	no requirement	In within Data Center building, provided with minimum 2 hour fire separation from all other areas	separate building or exterior weatherproof enclosures with Code required building separation	T4		
TIA	1	62	TIA.1.62	Data Center (Architectural)	Generator and fuel storage areas	Proximity to publicly accessible areas	no requirement	no requirement	9 m / 30 ft or greater separation	19 m / 60 ft or greater separation	T2		
TIA	2	1	TIA.2.1	Data Center (Security)	Security	System CPU UPS capacity	na	Building	Building	Building + Battery (8 hour min)	T3		
TIA	2	2	TIA.2.2	Data Center (Security)	Security	Data Gathering Panels (Field Panels) UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)	T4	Security systems on building UPS	
TIA	2	3	TIA.2.3	Data Center (Security)	Security	Field Device UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)	T4	Security systems on building UPS	
TIA	2	4	TIA.2.4	Data Center (Security)	Security	Security staffing per shift	na	1 per 3,000 sq m / 30,000 sq ft (1 minimum)	1 per 2,000 sq m / 20,000 sq ft (2 minimum)	1 per 2,000 sq m / 20,000 sq ft (3 minimum)	T2		
TIA	2	5	TIA.2.5	Data Center (Security)	Security Access Control Monitoring	Generators	industrial grade lock	intrusion detection	card access	card access	T1	plus camera coverage	
TIA	2	6	TIA.2.6	Data Center (Security)	Security Access Control Monitoring	UPS, Telephone & MEP Rooms	industrial grade lock	intrusion detection	card access	card access	T4		
TIA	2	7	TIA.2.7	Data Center (Security)	Security Access Control Monitoring	Fiber Vaults	industrial grade lock	intrusion detection	intrusion detection	card access	N/A	Owned/secured by Telco	
TIA	2	8	TIA.2.8	Data Center (Security)	Security Access Control Monitoring	Emergency Exit Doors	industrial grade lock	monitor	delay egress per code	delay egress per code	T2		
TIA	2	9	TIA.2.9	Data Center (Security)	Security Access Control Monitoring	Accessible Exterior Windows/opening	off site monitoring	intrusion detection (with offsite monitoring during shifts when no security staff is present)	intrusion detection (with offsite monitoring during shifts when no security staff is present)	intrusion detection	T4	Monitored by 24x7x365 on site security	
TIA	2	10	TIA.2.10	Data Center (Security)	Security Access Control Monitoring	Security Operations Center	no requirement	no requirement	card access	card access	T4		
TIA	2	11	TIA.2.11	Data Center (Security)	Security Access Control Monitoring	Network Operations Center	no requirement	no requirement	card access	card access	T4		
TIA	2	12	TIA.2.12	Data Center (Security)	Security Access Control Monitoring	Security Equipment Rooms	no requirement	intrusion detection	card access	card access	T4		
TIA	2	13	TIA.2.13	Data Center (Security)	Security Access Control Monitoring	Doors into Computer Rooms	industrial grade lock	intrusion detection	card or biometric access for ingress and egress	card or biometric access for ingress and egress	T4		
TIA	2	14	TIA.2.14	Data Center (Security)	Security Access Control Monitoring	Perimeter building doors	no monitoring	intrusion detection (with offsite monitoring during shifts when no security staff is present)	card access if main entrance, intrusion detection all others	card access all entrance	T3		
TIA	2	15	TIA.2.15	Data Center (Security)	Security Access Control Monitoring	Main door onto computer room floor	industrial grade lock	card access	Single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential	single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential, preferably with biometrics.	T2	no man trap but camera covered and biometric	
TIA	2	16	TIA.2.16	Data Center (Security)	Bullet resistant walls, windows & doors	Security Counter in Lobby	na	na	Level 3 (min)	Level 3 (min)	T2		

TIA	2	17	TIA.2.17	Data Center (Security)	Bullet resistant walls, windows & doors	Security Counter in Shipping and Receiving	na	na	na	Level 3 (min)	T3		
TIA	2	18	TIA.2.18	Data Center (Security)	CCTV Monitoring	Building perimeter and parking	no requirement	no requirement	yes	yes	T4		
TIA	2	19	TIA.2.19	Data Center (Security)	CCTV Monitoring	Generators	no requirement	no requirement	yes	yes	T4	access to mech yard covered	
TIA	2	20	TIA.2.20	Data Center (Security)	CCTV Monitoring	Access Controlled Doors	no requirement	yes	Yes	Yes	T4		
TIA	2	21	TIA.2.21	Data Center (Security)	CCTV Monitoring	Computer Room Floors	no requirement	no requirement	Yes	Yes	T4		
TIA	2	22	TIA.2.22	Data Center (Security)	CCTV Monitoring	UPS, Telephone & MEP Rooms	no requirement	no requirement	Yes	Yes	T2		
TIA	2	23	TIA.2.23	Data Center (Security)	CCTV	CCTV Recording of all activity on all cameras	no requirement	no requirement	Yes; digital	Yes; digital	T4		
TIA	2	24	TIA.2.24	Data Center (Security)	CCTV	Recording rate (frames per second)	no requirement	no requirement	20 frames/secs (min)	20 frames/secs (min)	T4		
TIA	3	1	TIA.3.1	Data Center (Structural)	Structural	Seismic zone -any zone acceptable although it may dictate more costly support mechanisms	no restriction	no restriction	no restriction	no restriction	T4		
TIA	3	2	TIA.3.2	Data Center (Structural)	Structural	Facility designed to seismic zone requirements	no restriction	no restriction	no restriction	In Seismic Zone 0, 1, 2 to Zone 3 requirements. In Seismic Zone 3 & 4 to Zone 4 requirements	T3		
TIA	3	3	TIA.3.3	Data Center (Structural)	Structural	Site Specific Response Spectra - Degree of local Seismic accelerations	no	no	with Operation Status after 10% in 50 year event	with Operation Status after 5% in 100 year event		No seismic risk in Phx	
TIA	3	4	TIA.3.4	Data Center (Structural)	Structural	Importance factor - assists to ensure greater than code design	I=1	I=1.5	I=1.5	I=1.5		No seismic risk in Phx	
TIA	3	5	TIA.3.5	Data Center (Structural)	Structural	Telecommunications equipment racks/cabinets anchored to base or supported at top and base	no	Base only	Fully braced	Fully braced		No seismic risk in Phx	
TIA	3	6	TIA.3.6	Data Center (Structural)	Structural	Deflection limitation on telecommunications equipment within limits acceptable by the electrical attachments	no	no	yes	yes	?	Do not understand the question	
TIA	3	7	TIA.3.7	Data Center (Structural)	Structural	Bracing of electrical conduits runs and cable trays	per code	per code w/ Importance	per code w/ Importance	per code w/ Importance	T1	No seismic risk in Phx	
TIA	3	8	TIA.3.8	Data Center (Structural)	Structural	Bracing of mechanical system major duct runs	per code	per code w/ Importance	per code w/ Importance	per code w/ Importance	T1	No seismic risk in Phx	
TIA	3	9	TIA.3.9	Data Center (Structural)	Structural	Floor loading capacity superimposed live load	7.2 kPa (150 lbf/sq ft).	8.4 kPa (175 lbf/sq ft)	12 kPa (250 lbf/sq ft)	12 kPa (250 lbf/sq ft)	T4		
TIA	3	10	TIA.3.10	Data Center (Structural)	Structural	Floor hanging capacity for ancillary loads suspended from below	1.2 kPa (25 lbf/sq ft)	1.2 kPa (25 lbf/sq ft)	2.4 kPa (50 lbf/sq ft)	2.4 kPa (50 lbf/sq ft)	N/A		
TIA	3	11	TIA.3.11	Data Center (Structural)	Structural	Concrete Slab Thickness at ground	127 mm (5 in)	127 mm (5 in)	127 mm (5 in)	127 mm (5 in)	T4		
TIA	3	12	TIA.3.12	Data Center (Structural)	Structural	Concrete topping over flutes for elevated floors	102 mm (4 in)	102 mm (4 in)	102 mm (4 in)	102 mm (4 in)	N/A		
TIA	3	13	TIA.3.13	Data Center (Structural)	Structural	affects size of anchor which can be installed	no requirement	no requirement	no requirement	no requirement	T4		
TIA	3	14	TIA.3.14	Data Center (Structural)	Structural	Building LFRS (Shearwall/Braced	Steel/Conc MF	Conc. Shearwall / Steel BF	Conc. Shearwall / Steel BF	Conc. Shearwall / Steel BF	T1	No seismic risk in Phx	
TIA	3	15	TIA.3.15	Data Center (Structural)	Structural	Building Energy Dissipation -Passive	none	none	Passive Dampers	Passive Dampers/Base Isolation	T2	No seismic risk in Phx	
TIA	3	16	TIA.3.16	Data Center (Structural)	Structural	Battery/UPS floor vs. building composition. Concrete floors more difficult to upgrade for intense loads. Steel framing with metal deck and fill much more easily upgraded.	PT concrete	CIP Mild Concrete	Steel Deck & Fill	Steel Deck & Fill	T4	Concrete and rebar	
TIA	3	17	TIA.3.17	Data Center (Structural)	Structural	Steel Deck & Fill/ PT concrete/ CIP Mild -slabs much more difficult to install anchors	PT	PT concrete	CIP Mild Concrete	Steel Deck & Fill	T4	Concrete and rebar	
TIA	4	1	TIA.4.1	Data Center (Electrical)	General	System allows concurrent maintenance	No	Down to but not including UPS output panelboard	Down to but not including power distribution unit	Throughout distribution system	T2		
TIA	4	2	TIA.4.2	Data Center (Electrical)	General	Single Points of Failure	One or more single points of failure for distribution systems serving electrical equipment or mechanical systems	One or more single points of failure for distribution systems serving electrical equipment or mechanical systems	No single points of failure for distribution systems serving electrical equipment or mechanical systems	No single points of failure for distribution systems serving electrical equipment or mechanical systems	T2		

TIA	4	3	TIA.4.3	Data Center (Electrical)	General	Power System Analysis	Short Circuity Study Coordination Study Arc Flash Analysis	Short Circuity Study Coordination Study Arc Flash Analysis	Short Circuity Study Coordination Study Arc Flash Analysis Load Flow Study	Short Circuity Study Coordination Study Arc Flash Analysis Load Flow Study	?	We do not do Arc Flash analysis	
TIA	4	4	TIA.4.4	Data Center (Electrical)	General	Computer & Telecommunications Equipment Power Cords	Single Cord Feed with 100% capacity	Single Cord Feed with 100% capacity	Redundant Cord Feed with 100% capacity on remaining cord or cords	Redundant Cord Feed with 100% capacity on remaining cord or cords	T4		
TIA	4	5	TIA.4.5	Data Center (Electrical)	Utility	Utility Entrance	Single Feed	Single Feed	N+1 Redundant Feed	2N Redundant Feed from different utility substations	T3		
TIA	4	6	TIA.4.6	Data Center (Electrical)	Main Utility Switchboard	Service	Shared	Dedicated	Dedicated	Dedicated	T4		
TIA	4	7	TIA.4.7	Data Center (Electrical)	Main Utility Switchboard	Construction	Panelboard with bolt on circuit breakers Optional	Panelboard with bolt on circuit breakers Optional	Panelboard with bolt on circuit breakers	Panelboard with bolt on circuit breakers	T4		
TIA	4	8	TIA.4.8	Data Center (Electrical)	Main Utility Switchboard	Surge Suppression	Optional	Optional	Yes	Yes	T4		
TIA	4	9	TIA.4.9	Data Center (Electrical)	Uninterruptible Power Supply Systems	Redundancy	N	N+1	N+1	2N	T3		
TIA	4	10	TIA.4.10	Data Center (Electrical)	Uninterruptible Power Supply Systems	Topology	Single or Parallel Modules	Single or Parallel Modules with static bypass	Parallel Redundant Modules or Distributed Redundant Modules or Block Redundant System	Parallel Redundant Modules or Distributed Redundant Modules or Block Redundant System	T4		
TIA	4	11	TIA.4.11	Data Center (Electrical)	Uninterruptible Power Supply Systems	Automatic Bypass	None	Non dedicated maintenance bypass feeder to UPS output switchboard	Dedicated maintenance bypass feeder to UPS output switchboard	Dedicated maintenance bypass feeder to UPS output switchboard	T4		
TIA	4	12	TIA.4.12	Data Center (Electrical)	Uninterruptible Power Supply Systems	Output Power Distribution	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating circuit breakers that are coordinated under overload and ground fault current condition	Panelboard incorporating circuit breakers that are coordinated under overload and ground fault current condition	T4		
TIA	4	13	TIA.4.13	Data Center (Electrical)	Uninterruptible Power Supply Systems	Battery String	Common String for multiple modules	Dedicated String for each module	Dedicated String for each module	Dedicated String for each module	T4		
TIA	4	14	TIA.4.14	Data Center (Electrical)	Uninterruptible Power Supply Systems	Battery type	5 year valve regulated lead acid	10 year valve regulated lead acid or flooded type	15 year valve regulated lead acid or flooded type	20 year lead acid flooded type			
TIA	4	15	TIA.4.15	Data Center (Electrical)	Uninterruptible Power Supply Systems	Battery Minimum Back Up Time	5 minutes	7 minutes	10 minutes	15 minutes	T4		
TIA	4	16	TIA.4.16	Data Center (Electrical)	Uninterruptible Power Supply Systems	Battery Monitoring System	Optional	Optional	String level by UPS system	Centralized automated system to check each cell for, voltage, and impedance or resistance	T3		
TIA	4	17	TIA.4.17	Data Center (Electrical)	Uninterruptible Power Supply Systems	Flywheel	Allowed	Allowed	Allowed	Allowed	N/A		
TIA	4	18	TIA.4.18	Data Center (Electrical)	Uninterruptible Power Supply Systems	Transformer	Optional	K-Rated or Harmonic Canceling	K-Rated or Harmonic Canceling Front Accessible for Maintenance	K-Rated or Harmonic Canceling Front Accessible for Maintenance	T4		
TIA	4	19	TIA.4.19	Data Center (Electrical)	Automatic Static Transfer Switch	Overcurrent Device	N/A	Fuse	Circuit Breaker	Circuit Breaker	T4		
TIA	4	20	TIA.4.20	Data Center (Electrical)	Automatic Static Transfer Switch	Maintenance Bypass Procedure	N/A	Manual Non Guided	Manual Guided	Manual Guided	T1 ?	Elec. Engineer contractor led shut down procedure	
TIA	4	21	TIA.4.21	Data Center (Electrical)	Automatic Static Transfer Switch	Output	N/A	Single Circuit Breaker	Dual Circuit Breaker	Dual Circuit Breaker	T2		
TIA	4	22	TIA.4.22	Data Center (Electrical)	Grounding	Lighting protection system	Based on risk analysis as per NFPA 780 and insurance requirements.	Based on risk analysis as per NFPA 780 and insurance requirements.	Yes	Yes	T4		
TIA	4	23	TIA.4.23	Data Center (Electrical)	Grounding	Service entrance grounds and generator grounds fully conform to NEC	Yes	Yes	Yes	Yes	T4		
TIA	4	24	TIA.4.24	Data Center (Electrical)	Grounding	Lighting fixtures neutral isolated from service entrance derived from lighting transformer for ground fault isolation	No	No	Yes	Yes	T4		
TIA	4	25	TIA.4.25	Data Center (Electrical)	Grounding	Data center grounding infrastructure in computer room	Optional	Optional	Yes	Yes	T4		
TIA	4	26	TIA.4.26	Data Center (Electrical)	Computer Room Emergency Power Off (EPO) System	Installation	Do not install if not required by authorities having jurisdiction	Do not install if not required by authorities having jurisdiction	Do not install if not required by authorities having jurisdiction	Do not install if not required by authorities having jurisdiction	T4	We do have EPO installed	
TIA	4	27	TIA.4.27	Data Center (Electrical)	Computer Room Emergency Power Off (EPO) System	Test Mode	Optional	Optional	Yes	Yes	T2		
TIA	4	28	TIA.4.28	Data Center (Electrical)	Computer Room Emergency Power Off (EPO) System	Alarm	Optional	Optional	Yes	Yes	T4		
TIA	4	29	TIA.4.29	Data Center (Electrical)	Computer Room Emergency Power Off (EPO) System	Abort Swtich	Optional	Optional	Yes	Yes	T2	Have EPO enable for life safety	

TIA	4	30	TIA.4.30	Data Center (Electrical)	Central Power Monitoring	Monitored Points	None	Utility UPS Generator	Main Transformer UPS Generator Feeder Circuit Breakers Automatic Static Transfer Switch PDU Automatic Transfer Switches	Main Transformer UPS Generator Feeder Circuit Breakers Automatic Static Transfer Switch PDU Automatic Transfer Switches	T2		
TIA	4	31	TIA.4.31	Data Center (Electrical)	Central Power Monitoring	Notification Method	N/A	Control Room Console	Control Room Console Pager Email Text Message	Control Room Console Pager Email Text Message	T2	d 24x7x365, escalation driven from monitoring personnel	
TIA	4	32	TIA.4.32	Data Center (Electrical)	Battery Room	Separate from UPS/Switchgear Equipment Rooms	No	Yes	Yes	Yes	T4		
TIA	4	33	TIA.4.33	Data Center (Electrical)	Battery Room	Individual Battery Strings Isolated from Each Other	No	Yes	Yes	Yes	T1		
TIA	4	34	TIA.4.34	Data Center (Electrical)	Battery Room	Shatterproof Viewing Glass in Battery Room Door	No	No	No	Yes	T3		
TIA	4	35	TIA.4.35	Data Center (Electrical)	Standby Generating System	Generator Sizing	Sized for UPS System only	Sized for UPS & mechanical system	Sized for total building load N+1 redundancy	Sized for total building load with 2N redundancy	T3		
TIA	4	36	TIA.4.36	Data Center (Electrical)	Standby Generating System	Generators on Single Bus	Yes	Yes	Yes	No	T3		
TIA	4	37	TIA.4.37	Data Center (Electrical)	Loadbank	Installation	None	Provision for Portable	Provision for Portable	Permanent	T3		
TIA	4	38	TIA.4.38	Data Center (Electrical)	Loadbank	Equipment Tested	N/A	Generater	Generator UPS	Generator UPS	T4		
TIA	4	39	TIA.4.39	Data Center (Electrical)	Loadbank	Auto Shutdown	N/A	None	Automatic upon failure of utility	Automatic upon failure of utility	T4		
TIA	4	40	TIA.4.40	Data Center (Electrical)	Testing	Factory Acceptance Testing	Optional	Optional	Yes	Yes	T4		
TIA	4	41	TIA.4.41	Data Center (Electrical)	Testing	Site Circuit breaker testing	Optional	Optional	Contact Resistance test of all circuit breakers in critical and essential paths, 225 Amps and higher	Contact Resistance test of all circuit breakers in critical and essential paths, 225 Amps and higher	T2		
TIA	4	42	TIA.4.42	Data Center (Electrical)	Testing	Commissioning	Optional	Component level System level	Component level System level Integrated System	Component level System level Integrated System	T4	For new install or upgrade of critical power infrastructure	
TIA	4	43	TIA.4.43	Data Center (Electrical)	Equipment Maintenance	Maintenance Staff	Onsite Day Shift only. On-call at other times	Onsite Day Shift only. On-call at other times	Onsite 24 hrs M-F, on-call on weekends	Onsite 24/7	T2		
TIA	4	44	TIA.4.44	Data Center (Electrical)	Equipment Maintenance	Preventative Maintenance	None	None	Limited preventative maintenance program	Comprehensive preventative maintenance program	T4		
TIA	5	1	TIA.5.1	Data Center (Electrical)	Equipment Maintenance	Facility Training Programs	None	None	Comprehensive training program	Comprehensive training program including manual operation procedures if it is necessary to bypass control system	T3		
TIA	5	2	TIA.5.2	Data Center (Mechanical)	General	Routing of water or drain piping not associated with the data center equipment in data center spaces	Permitted but not recommended	Permitted but not recommended	Not permitted	Not permitted	T4		
TIA	5	3	TIA.5.3	Data Center (Mechanical)	General	Positive pressure in computer room and associated spaces relative to outdoors and non-data center spaces	No requirement	Yes	Yes	Yes	T4		
TIA	5	4	TIA.5.4	Data Center (Mechanical)	General	Floor drains in computer room for condensate drain water, humidifier flush water, and sprinkler discharge water	Yes	Yes	Yes	Yes	T4		
TIA	5	5	TIA.5.5			Mechanical systems on standby generator	No requirement	Yes	Yes	Yes	T4		
TIA	5	6	TIA.5.6	Data Center (Mechanical)	Water-Cooled System	Indoor Terminal Air Conditioning Units	No redundant air conditioning units	One redundant AC Unit per critical area	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	7	TIA.5.7	Data Center (Mechanical)	Water-Cooled System	Humidity Control for Computer Room	No requirements	Humidification provided	Humidification provided	Humidification provided	T4		

TIA	5	8	TIA.5.8	Data Center (Mechanical)	Water-Cooled System	Electrical Service to Mechanical Equipment	Single path of electrical power to AC equipment	Single path of electrical power to AC equipment	Multiple paths of electrical power to AC equipment. Connected in checkerboard fashion for cooling redundancy	Multiple paths of electrical power to AC equipment. Connected in checkerboard fashion for cooling redundancy	T3	of "checkerboard" definition but we have dual feeds.	
TIA	5	9	TIA.5.9	Data Center (Mechanical)	Water-Cooled System Heat Rejection	Dry-coolers (where applicable)	No redundant dry coolers	One redundant dry cooler per system	Qty. of dry coolers sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of dry coolers sufficient to maintain critical area during loss of one source of electrical power	N/A		
TIA	5	10	TIA.5.10	Data Center (Mechanical)	Water-Cooled System Heat Rejection	Closed-Circuit Fluid Coolers (where applicable)	No redundant fluid coolers	One redundant fluid cooler per system	Qty. of dry coolers sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of fluid coolers sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	11	TIA.5.11	Data Center (Mechanical)	Water-Cooled System Heat Rejection	Circulating Pumps	No redundant condenser water pumps	One redundant condenser water pump per system	Qty. of dry coolers sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of condenser water pumps sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	12	TIA.5.12	Data Center (Mechanical)	Water-Cooled System Heat Rejection	Piping System	Single path condenser water system	Single path condenser water system	Headered parallel piped condenser water system	Dual path condenser water system	T2		
TIA	5	13	TIA.5.13	Data Center (Mechanical)	Chilled Water System	Indoor Terminal Air Conditioning Units	No redundant air conditioning units	One redundant AC Unit per critical area	Qty. of AC Units sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	14	TIA.5.14	Data Center (Mechanical)	Chilled Water System	Humidity Control for Computer Room	No requirements	Humidification provided	Humidification provided	Humidification provided	T4		
TIA	5	15	TIA.5.15	Data Center (Mechanical)	Chilled Water System	Electrical Service to Mechanical Equipment	Single path of electrical power to AC equipment	Single path of electrical power to AC equipment	Multiple paths of electrical power to AC equipment	Multiple paths of electrical power to AC equipment	T4		
TIA	5	16	TIA.5.16	Data Center (Mechanical)	Chilled Water System Heat Rejection	Chilled Water Piping System	Single path chilled water system	Single path chilled water system	Dual path ladder loop chilled water system with isolation valves	Dual path chilled water system	T2		
TIA	5	17	TIA.5.17	Data Center (Mechanical)	Chilled Water System Heat Rejection	Chilled Water Pumps	No redundant chilled water pumps	One redundant chilled water pump per system	Qty. of chilled water pumps sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of chilled water pumps sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	18	TIA.5.18	Data Center (Mechanical)	Chilled Water System Heat Rejection	Air-Cooled Chillers	No redundant chiller	One redundant chiller per system	Qty. of chilled water pumps sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of chillers sufficient to maintain critical area during loss of one source of electrical power	N/A		
TIA	5	19	TIA.5.19	Data Center (Mechanical)	Chilled Water System Heat Rejection	Water-cooled Chillers	No redundant chiller	One redundant chiller per system	Qty. of chilled water pumps sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of chillers sufficient to maintain critical area during loss of one source of electrical power	N/A		
TIA	5	20	TIA.5.20	Data Center (Mechanical)	Chilled Water System Heat Rejection	Cooling Towers	No redundant cooling tower	One redundant cooling tower per system	Qty. of chilled water pumps sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of cooling towers sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	21	TIA.5.21	Data Center (Mechanical)	Chilled Water System Heat Rejection	Condenser Water Pumps	No redundant condenser water pumps	One redundant condenser water pump per system	Qty. of chilled water pumps sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of condenser water pumps sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	22	TIA.5.22	Data Center (Mechanical)	Chilled Water System Heat Rejection	Condenser Water Piping System	Single path condenser water system	Single path condenser water system	Headered parallel piped condenser water system	Dual path condenser water system	T2		

TIA	5	23	TIA.5.23	Data Center (Mechanical)	Air-Cooled System	Indoor Terminal Air Conditioning Units/Outdoor Condensers	No redundant air conditioning units	One redundant AC Unit per critical area	Qty. of AC Units sufficient to provide minimal temporary capacity to critical area during loss of one source of electrical power	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power	T4		
TIA	5	24	TIA.5.24	Data Center (Mechanical)	Air-Cooled System	Electrical Service to Mechanical Equipment	Single path of electrical power to AC equipment	Single path of electrical power to AC equipment	Multiple paths of electrical power to AC equipment	Multiple paths of electrical power to AC equipment			
TIA	5	25	TIA.5.25	Data Center (Mechanical)	Air-Cooled System	Humidity Control for Computer Room	No requirements	Humidification provided	Humidification provided	Humidification provided	T4		
TIA	5	26	TIA.5.26	Data Center (Mechanical)	HVAC Control System	HVAC Control System	Control system failure will interrupt cooling to critical areas	Control system failure will not interrupt cooling to critical areas	Control system failure will not interrupt cooling to critical areas	Control system failure will not interrupt cooling to critical areas	T4		
TIA	5	27	TIA.5.27	Data Center (Mechanical)	HVAC Control System	Power Source to HVAC Control System	Single path of electrical power to HVAC control system	Redundant, UPS electrical power to BMS Control	Redundant, UPS electrical power to BMS Control	Redundant, UPS electrical power to BMS Control	T4		
TIA	5	28	TIA.5.28	Data Center (Mechanical)	Plumbing (for water-cooled heat rejection)	Water	Single water supply, with no on-site back-up storage	Dual sources of water, or one source + on-site storage	Dual sources of water, or one source + on-site storage	Dual sources of water, or one source + on-site storage	T1		
TIA	5	29	TIA.5.29	Data Center (Mechanical)	Plumbing (for water-cooled heat rejection)	Points of Connection to Condenser Water System	Single point of connection	Single point of connection	Two points of connection	Two points of connection			
TIA	5	30	TIA.5.30	Data Center (Mechanical)	Fuel Oil System	Bulk Storage Tanks	Single storage tank	Single storage tanks	Multiple storage tanks	Multiple storage tanks	T4		
TIA	5	31	TIA.5.31	Data Center (Mechanical)	Fuel Oil System	Storage Tank Pumps and Piping	Single pump and/or supply pipe	Multiple pumps, multiple supply pipes	Multiple pumps, multiple supply pipes	Multiple pumps, multiple supply pipes	T4		
TIA	5	32	TIA.5.32	Data Center (Mechanical)	Fire Suppression	Fire detection system	no	yes	yes	yes	T4		
TIA	5	33	TIA.5.33	Data Center (Mechanical)	Fire Suppression	Fire sprinkler system	When required	Pre-action (when required)	Pre-action (when required)	Pre-action (when required)	T4		
TIA	5	34	TIA.5.34	Data Center (Mechanical)	Fire Suppression	Gaseous suppression system	no	no	clean agents listed in NFPA 2001	clean agents listed in NFPA 2001	T4	Halon	
TIA	5	35	TIA.5.35	Data Center (Mechanical)	Fire Suppression	Early Warning Smoke Detection System	no	yes	yes	yes	T4		
TIA	5	36	TIA.5.36	Data Center (Mechanical)	Fire Suppression	Water Leak Detection System	no	yes	yes	yes	T4		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Infrastructure

Base	Level	Sub	ReqID New	Focus	Specifics	RequirementDescription	Requirement Fulfilled?	Notes	Evidence
H2	1	1	H2.1.1	Infrastructure	General	Hosting Provider will deliver infrastructure and related services from within its approved Data Centers.	Y		
H2	1	2	H2.1.2	Infrastructure	General	Hosting Provider infrastructure will consist of dedicated servers, operating systems, local area network equipment, firewalls, routers, load balancers and any related equipment or provided software	Y		
H2	1	3	H2.1.3	Infrastructure	General	Hosting Provider is solely responsible for procuring, managing and maintaining infrastructure, whether within Hosting Provider's Data Centers or Hosting Provider equipment deployed at Customer sites.	Y		
H2	1	4	H2.1.4	Infrastructure	General	Hosting Provider is also be solely responsible for acquiring and maintaining Wide Area Network (WAN) connectivity between Customer's site and Hosting Provider's Data Centers.	Y		
H2	1	5	H2.1.5	Infrastructure	General	Hosting Provider infrastructure applies to Production Environments, Production Support Environments, and Non-Production Environments managed for Customer.	Y		
H2	1	6	H2.1.6	Infrastructure	Acqusition and Provisioning	The Infrastructure Design Document and the Provisioning Release Plan will be used as the basis to install and configure the hardware, network, storage and software required for the environments.	Y		
H2	1	7	H2.1.7	Infrastructure	Acqusition and Provisioning	Hosting Provider will procure, install, and configure the required hardware in accordance with the Provisioning Release Plan	Y		
H2	1	8	H2.1.8	Infrastructure	Acqusition and Provisioning	Hosting Provider will install Hosting Provider's Certified Configuration onto each provisioned Server	Y		
H2	1	9	H2.1.9	Infrastructure	Acqusition and Provisioning	Hosting Provider will provide a VPN devices to be installed within Customer's internal network; or, allow installation of the Hosting Provider-approved Customer-provided Network Equipment in accordance with the network architecture solution approved by Hosting Provider	Y		
H2	1	10	H2.1.10	Infrastructure	Acqusition and Provisioning	Hosting Provider will Provide Internal IP address management, router table management, switch administration and firewall administration within Hosting Provider's Data Center(s)	Y		
H2	1	11	H2.1.11	Infrastructure	Acqusition and Provisioning	Hosting Provider will enable "public" Internet access for the applicable Hosting Provider Programs per the Provisioning Release Plan, and install a DMZ Server(s) per the Infrastructure Requirements Document	Y		
H2	1	12	H2.1.12	Infrastructure	Acqusition and Provisioning	Hosting Provider will install and manage required Third Party Software	Y		
H2	1	13	H2.1.13	Infrastructure	Acqusition and Provisioning	Hosting Provider will ensure implementation/deployment plans are aligned with the Provisioning Release Plan	Y		
H2	1	14	H2.1.14	Infrastructure	Availability Management	Hosting Provider will provide Availability Management which is the measurement and management of infrastructure, including measurement of service failures and the time taken to resume service.	Y		
H2	1	15	H2.1.15	Infrastructure	Availability Management	Hosting Provider will utilize monitoring Tools to identify actual or potential Incidents affecting availability and take action to prevent or minimize such impact. State must be notified when incidents are identified effecting application availability.	Y		
H2	1	16	H2.1.16	Infrastructure	Availability Management	Hosting Provider will perform Problem Management analysis and make recommendations to Customer of activities that may enhance service quality and reduce recurrence of Incidents affecting availability	Y		
H2	1	17	H2.1.17	Infrastructure	Availability Management	Hosting Provider will maintain availability for software products not provided by Hosting Provider	Y (CGI managed products only)		
H2	1	18	H2.1.18	Infrastructure	Availability Management	Hosting Provider will manage ISP/Network connectivity between Customer's Data Center and Hosting Provider's Data Center	Y (configured to support HBE needs)		
H2	1	19	H2.1.19	Infrastructure	General	Hosting Provider solution will utilize industry standard hardware(storage, servers, switches, firewalls, load balancers).	Y		
H2	1	20	H2.1.20	Infrastructure	General	Hosting Provider will utilze industry standard virtualization technology and deploy following vendors best practices.	Y		
H2	1	21	H2.1.21	Infrastructure	General	Hosting Provider will build Customers private cloud utilizing dedicated physical and virtual separation and components.	Y		
H2	1	22	H2.1.22	Infrastructure	Design	Hosting Provider will assist Customer in preparing the detailed infrastructure requirements	Y		
H2	1	23	H2.1.23	Infrastructure	Design	Hosting Provider will utilize Customer requirements to design the Hosting Provider Services architecture and prepare an Infrastructure Design Document.	Y		
H2	1	24	H2.1.24	Infrastructure	Design	Hosting Provider will prepare a Provisioning Release Plan and review the plan with Customer	Y		
H2	1	25	H2.1.25	Infrastructure	Design	Hosting Provider will provide Customer with network capacity recommendations for connectivity between Hosting Provider's Data Center and Customer's premises	Y		
H2	1	26	H2.1.26	Infrastructure	Design	Hosting Provider solution architecture including physical and virtual infrastructure, firewall, load balancers, etc. proposed for individual production and non-production environments will be produced by Customer and approved by Hosting Provider. (refer to visio Customer Environment Diagrams (Production, Disaster Recovery, Staging, Testing, etc.)	Y		
H2	1	27	H2.1.27	Infrastructure	Design	Hosting Provider will Collect and document, and publish all infrastructure/environments under Hosting Provider management	Y		
H2	1	28	H2.1.28	Infrastructure	Environments	Hosting Provider will implement a high available Production Environment per Customers Production, Environment Diagram.	Y		
H2	1	29	H2.1.29	Infrastructure	Environments	(PRODUCTION) Hosting Provider will implement a high available Production Environment per Customers Production Environment Diagram.	Y		
H2	1	30	H2.1.30	Infrastructure	Environments	(STAGING) Hosting Provider will implement a high available Staging Environment (mirrors PRODUCTION) per Customers Staging Environment Diagram.	Y		
H2	1	31	H2.1.31	Infrastructure	Environments	(DISASTER RECOVERY(DR)) Hosting Provider will implement a high available DR Environment (mirrors PRODUCTION) per Customers DR Environment Diagram.	Y		
H2	1	32	H2.1.32	Infrastructure	Environments	(TEST) Hosting Provider will implement a Non high available TEST Environment per Customers TEST Environment Diagram. Non Production environments will be design at the same level of security as PRODUCTION and will contain the same applications and services as PRODUCTION without the high availability requirements.	Y		
H2	1	33	H2.1.33	Infrastructure	Environments	(DEV) Hosting Provider will implement a Non high available DEV Environment per Customers DEV Environment Diagram. Non Production environments will be design at the same level of security as PRODUCTION and will contain the same applications and services as PRODUCTION without the high availability requirements.	Y		

H2	1	34	H2.1.34	Infrastructure	Environments	(TRAINING) Hosting Provider will implement a Non high available TRAINING Environment per Customers TRAINING Environment Diagram. Non Production environments will be design at the same level of security as PRODUCTION and will contain the same applications and services as PRODUCTION without the high availability requirements.	Y		
H2	1	35	H2.1.35	Maintenance and Operations	Design	The Application Server shall be a scalable, enterprise-ready application and shall support the deployment of many types of distributed applications and provides an ideal foundation for building applications based on Service Oriented Architectures (SOA)	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Networking

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H3	1	1	H3.1.1	Network	Bandwidth	Bandwidth refers to the amount of traffic to be carried through a network and should be considered when designing Network Connectivity. The required bandwidth depends on the programs, number of concurrent users, and use of the programs. Network bandwidth must be monitored and adjusted as program usage grows and changes.	Y		
H3	1	2	H3.1.2	Network	Bandwidth	Bandwidth requirements for deployments vary depending on the programs used, Customer's business, and Customer's workflow. Hosting Provider will recommend the bandwidths as a starting point for network sizing deployment.	Y		
H3	1	3	H3.1.3	Network	Design	Hosting Provider is responsible for the network design and must provide network connection configuration, including a detailed cabling diagram for the network connections between Customer and Hosting Provider data center locations.	Y		
H3	1	4	H3.1.4	Network	Design	Hosting Provider shall provide public Internet addresses for devices that require Internet access, and Hosting Provider shall provide public addresses for equipment interfaces that connect to the Hosting Provider network.	Y		
H3	1	5	H3.1.5	Network	Design	If the Environment is supported by the (Hosting Provider Internal Service Network (HPISN)), all access into the Environment must traverse a firewall designed to validate the communications being attempted. The firewall performs this validation by recognizing protocols and verifying the acceptability of ranges of source and destination IP addresses.	Y		
H3	1	6	H3.1.6	Network	DMZ	If Customer chooses to access the Hosting Provider Programs via the public Internet, service will be deployed on DMZ Server(s) for Hosting Provider Managed Applications.	Y		
H3	1	7	H3.1.7	Network	DMZ	Hosting Provider Programs accessible from the public Internet shall be deployed on DMZ Servers for Hosting Provider Managed applications.	Y		
H3	1	8	H3.1.8	Network	DNS	Hosting Provider DNS Standards require the use of a CNAME alias in Customer's external DNS rather than an A record to the IP address to prevent the need for future modifications on Customer's side. This is required so that Hosting Provider can change the server IP addresses as required due to upgrades, relocations, and disaster recovery operations.	Y		
H3	1	9	H3.1.9	Network	DNS	For Hosting Provider personnel to support the Hosting Provider Programs, the applications URL or hostnames must be resolvable in Customer's external DNS.	Y		
H3	1	10	H3.1.10	Network	DNS	Hosting Provider will not utilize hidden or split DNS solutions that impede operations, complicate support and are not valid security solutions.	Y		
H3	1	11	H3.1.11	Network	DNS	Hosting Provider will not utilize DNS sub-domain registrations. Hosting Provider follows and supports RFC 1178, RFC 952, and RFC 987 for hostname registration.	Y		
H3	1	12	H3.1.12	Network	DNS	Hosting Provider shall register the hostnames on an individual basis as part of the HPISN DNS Servers so that Hosting Provider does not have to use hostname entries on the desktop, and Hosting Provider can enforce accountability for hosts that are supported at Customer's site.	Y		
H3	1	13	H3.1.13	Network	DNS	Hosting Provider will configure the DNS to use the default Hosting Provideroutsourcing.com domain for application URLs, for example Customer.Hosting Provideroutsourcing.com. This URL is registered as a canonical name (CNAME) DNS record pointing to the Server address assigned to the Customer URL.	Y		
H3	1	14	H3.1.14	Network	DNS	Hosting Provider shall maintain both the A and the CNAME record on Hosting Provider DNS servers. Host and Domain Name DNS Record Type Data Values.	Y		
H3	1	15	H3.1.15	Network	DNS	Customer may use its own domain for its URL, such as portal.company.com. (This is accomplished with a CNAME record entry on Customer's DNS server and an A record on Hosting Provider's DNS servers.)	Y		
H3	1	16	H3.1.16	Network	General	Customer shall access the Hosting Provider Programs through a URL entered in a Web browser. A DNS server converts the URL to an IP address. For example, to access Hosting Provider's home page, Customer may enter http://www.Hosting Provider.com in a Web browser. Customer's computer asks its DNS server for the IP address associated with www.Hosting Provider.com and the browser then attempts to connect to the Web server at that IP address.	Y		
H3	1	17	H3.1.17	Network	General	Properly configured and sized network routers typically induce little delay. However, the delay through routers can become a major source of overall network latency when network connections are congested or routers are improperly configured. Hosting Provider will ensure that all network devices and links are properly sized and configured and are running optimally.	Y		
H3	1	18	H3.1.18	Network	Hosting Provider Internal Service Network	Hosting Provider (Hosting Provider Internal Service Network (HPISN)) will use firewall, VPN and syslog information to report on Hosting Provider personnel activity. The information captured in the report includes the following: User ID, User IP address by VPN concentrator, IP of system to which the user is connecting to, duration of the connection (in seconds), date and time.	Y		
H3	1	19	H3.1.19	Network	Hosting Provider Internal Service Network	All Hosting Provider personnel must connect to the HPISN using a software VPN client. After the Hosting Provider employee initiates a software VPN session, the employee must enter a user name and password. When authentication is successful, the Hosting Provider employee is assigned a static IP address for that particular VPN concentrator. The IP addresses are bound to the user identity and not, for example, to the MAC address. IP spoofing and other threats are reduced because the client software enforces the IP assigned by the authentication server.	Y		
H3	1	20	H3.1.20	Network	Hosting Provider Internal Service Network	Hosting Provider HPISN is designed to provide appropriate Hosting Provider personnel secure network access to Servers used to provide Hosting Provider Services.	Y		
H3	1	21	H3.1.21	Network	Hosting Provider Internal Service Network	Hosting Provider maintains a dedicated support network (Hosting Provider Internal Support Network(HPISN)) that is segregated from Hosting Provider's Intranet. The network is comprised of a firewall, VPN, intrusion detection, authentication, reporting, and DNS. This isolated network is the standard Network Connectivity option for Hosting Provider personnel to connect to the Environment.	Y		
H3	1	22	H3.1.22	Network	Hosting Provider Internal Service Network	The HPISN utilizes redundant firewalls, intrusion detection systems (IDS), syslog and VPN technologies to secure the Environment. Default-deny rule sets are enforced by the firewall security policy and an IDS monitors any potential violations of the predefined rules. In addition, a third party assessment vendor performs periodic assessments of the Environment.	Y		
H3	1	23	H3.1.23	Network	Hosting Provider Internal Service Network	The HPISN architecture assigns static IP addresses to individual Hosting Provider personnel. As each user IP passes through the HPISN firewalls, Hosting Provider logs and reports the session activity to the Environment.	Y		
H3	1	24	H3.1.24	Network	Hosting Provider Internal Service Network	Hosting Provider is responsible for access control into Hosting Provider's Data Centers and to the Environment. This access control is designed to limit access to the Environment to Customer's network connections.	Y		
H3	1	25	H3.1.25	Network	Hosting Provider Internal Service Network	Hosting Provider personnel shall utilize the HPISN to connect to servers located at Customer's Data Center. Customer is responsible for access control into Customer's Data Center.	Y		

H3	1	26	H3.1.26	Network	Hosting Provider Internal Service Network	Hosting Provider personnel connect to the Data Center(s) using the HPISN dedicated support network.	Y		
H3	1	27	H3.1.27	Network	IDS	Hosting Provider employs IDS to provide continuous surveillance for intercepting and responding to security events as they are identified. Hosting Provider utilizes a network-based monitoring approach to detect attacks on open-firewalls ports. Events are analyzed using signature detection, which is a pattern matching of systems settings and user activities against a database of known attacks. Hosting Provider updates the signature database as updates become available. Alerts are forwarded to Hosting Provider's IT security and the Hosting Provider Service Desk for review and response to potential threats.	Y		
H3	1	28	H3.1.28	Network	IP addresses	HPISN syslog reports show individual IP addresses of users that access the Environment. Hosting Provider captures the individual user IP address information in syslog before the address is translated to Customer. Customer may request a syslog report on a monthly basis.	Y		
H3	1	29	H3.1.29	Network	IP addresses	Hosting Provider can send the IP addresses of Hosting Provider personnel to Customer, encapsulated in subnet ranges.	Y		
H3	1	30	H3.1.30	Network	IP Addresses	Hosting Provider will ensure that only routable IP addresses are presented to Hosting Provider	Y		
H3	1	31	H3.1.31	Network	IP Addresses	Hosting Provider will specify IP addresses to route to Hosting Provider's Data Center(s)	Y		
H3	1	32	H3.1.32	Network	IP addresses	Hosting Provider shall recognize that the use of private addresses is a common practice. Network Address Translation (NAT) and Port Address Translation (PAT) can be used to map private addresses to public addresses. Hosting Provider will aid in providing the public IP addresses and for performing the NAT/PAT.	Y		
H3	1	33	H3.1.33	Network	IP addresses	One-to-one static NAT must be used for all network devices, including, without limitation, Customer's printers or print servers to which Hosting Provider will initiate a connection. PAT is allowed for any network device that initiates the connection with Hosting Provider, such as User workstations connecting to the Hosting Provider Programs.	Y		
H3	1	34	H3.1.34	Network	IP addresses	Hosting Provider will perform the required translations for NAT if used.	Y		
H3	1	35	H3.1.35	Network	IP addresses	Hosting Provider will provide a list of IP addresses for Customer to route over the Transaction Link or Management Link.	Y		
H3	1	36	H3.1.36	Network	IP addresses	To avoid IP address conflicts, Hosting Provider will only route network traffic to globally unique public IP addresses registered through one of the regional Internet registry organizations. Hosting Provider will not route traffic to private IP addresses	Y		
H3	1	37	H3.1.37	Network	Latency	Hosting Provider will utilize network providers that can provide circuits with documented latency from Customer's to Hosting Provider's U.S. Data Centers of less than 100ms from within the U.S.	Y		
H3	1	38	H3.1.38	Network	Metrics	Hosting Provider will provide recommendations for network metrics	Y		
H3	1	39	H3.1.39	Network	Monitoring	Hosting Provider will monitor network usage and resize as appropriate	Y		
H3	1	40	H3.1.40	Network	Performance	Hosting Provider must determine its peak usage for each program and continually monitor its network traffic. After determining the correct network capacity for peak loads, Hosting Provider will make recommendations to Customer to upgrade network links that exceed 80 percent of network capacity during peak usage.	Y		
H3	1	41	H3.1.41	Network	Performance	Hosting Provider will provide network circuits that meet Hosting Provider's recommended bandwidth, latency, and error rate to deliver Hosting Provider Services.	Y		
H3	1	42	H3.1.42	Network	Performance	Hosting Provider will provide Internet network circuits in accordance with Hosting Provider Data Center bandwidth and latency requirements	Y		
H3	1	43	H3.1.43	Network	Performance	All network links are subject to transmission errors such as dropped packets. A high error rate can lead to increased latency and poor network performance. Each segment in a network can experience independent errors that add to the total error rate for the entire link. To ensure that a network operates at peak performance, the end-to-end error rate should not exceed 0.01 percent.	Y (as a target)		
H3	1	44	H3.1.44	Network	Personnel	Hosting Provider authorization for Hosting Provider personnel to access the Environment is comprised of the following two components: Network authorization, System authorization.	Y		
H3	1	45	H3.1.45	Network	Routing	Hosting Provider will route traffic to Customer over the Transaction Link or Management Link, as applicable	Y		
H3	1	46	H3.1.46	Network	SSL	Hosting Provider shall deploy SSL for all Web-based applications for Hosting Provider deployments that involve Internet-facing deployments and for deployments that are accessible through a secure network, such as a hardware VPN. SSL must be used for data transmitted through all Hosting Provider Web-based applications.	Y		
H3	1	47	H3.1.47	Network	SSL	Hosting provider shall deploy non SSL-enabled applications privately and not expose them ot the public Internet. Such application shall be accessible through a secure network connection. Customer connections to non-Internet applications must use SSL and a secure network connection.	Y		
H3	1	48	H3.1.48	Network	SSL	Although Customer may choose to access its Web-based, SSL-enabled applications through the public Internet, Hosting Provider will recommend that Customer deploy such applications as non-Internet facing using SSL and a secure network connection, such as a hardware VPN.	Y		
H3	1	49	H3.1.49	Network	SSL	The Hosting Provider shall procure and renew SSL certificates on Customer's behalf.	Y		
H3	1	50	H3.1.50	Network	SSL	Hosting Provider uses server load balancers with built-in SSL accelerator functions. This architecture enables off loading of CPU-intensive SSL processing from the Web Servers and centralizes the location of Web site private keys and certificate files. This improves the performance of, and provides better security for, the Environment. SSL uses a serial data transfer, which means that it sequentially acknowledges receipt of each packet transferred. Because SSL decryption of data is dependent on client processor speed, a slow or overloaded desktop computer may impact application performance.	Y		
H3	1	51	H3.1.51	Network	WAN	Hosting Provider will recommend bandwidth for sizing the WAN link between Customer and Hosting Provider. If Customer has a WAN between Customer's locations, Hosting Provider will aid Customer in assessing the traffic requirement for each link and size the link appropriately.	Y		
H3	1	52	H3.1.52	Network	WAN	Hosting Provider establishes a dedicated circuit for Customer's Internet circuit that is only used for Hosting Provider Services. A dedicated circuit can help prevent problems related to over use by isolating traffic to Hosting Provider from Customer's other Internet traffic. A dedicated circuit can help achieve stable and predictable Network Connectivity.	Y (not using vt state internet)		
H3	1	53	H3.1.53	Network	WAN	Hosting Provider uses VPN devices in a site-to-site (network-to-network) topology leveraging the public Internet or dedicated links.	Y		
H3	1	54	H3.1.54	Network	WAN	Hosting Provider implements Internet Protocol Security (IPsec) as part of an overall VPN strategy to secure data between endpoints on the Management Link by employing tunneling and encryption to facilitate data privacy.	Y		
H3	1	55	H3.1.55	Network	WAN	Hosting Provider pre-configures an Hosting Provider-provided VPN(s) to provide the following levels of encryption and authentication, in accordance with the IPSec standard: Data encryption using 168-bit Triple Des or AES256, Hashed Message Authentication Codes (HMAC) with a SHA-1 algorithm.	Y		
H3	1	56	H3.1.56	Network	WAN	The standard Network Connectivity between Hosting Provider and Customer is through a hardware VPN provided by Hosting Provider.	Y		

H3	1	57	H3.1.57	Network	WAN	Hosting Provider will establish a network transport between Hosting Provider and Customer to allow Hosting Provider personnel access to the Environment (a "Management Link") if environments are deployed within Customer Data Centers.	Y		
H3	1	58	H3.1.58	Network	WAN	Hosting Provider will provide access to the Environment will be via a virtual private network (VPN) connection. Hosting Provider will provide Customer with the number and type of VPNs required:	Y		
H3	1	59	H3.1.59	Network	WAN	Hosting Provider establishes a an Internet circuit that is used both for Network Connectivity to Hosting Provider and Customer's other Internet activities is called a shared circuit. Hosting Provider must ensure that the existing circuit has enough unused capacity to support Hosting Provider traffic.	Y		
H3	1	60	H3.1.60	Network	WAN	A shared circuit to the Hosting Provider should only be considered for Transaction Links if the circuit performance is highly stable and actively monitored for performance and capacity.	Y		
H3	1	61	H3.1.61	Network	WAN	With the Hosting Provider standard VPN, Hosting Provider supplies, configures, and manages an IPSec compliant VPN device installed on Customer's network. Hosting Provider standard VPNs can be implemented in most Customer environments in a short time frame and receives the highest level of VPN support from Hosting Provider.	Y		
H3	1	62	H3.1.62	Network	WAN	Hosting Provider specifies, designs and delivers a network transport to allow Hosting Provider personnel to access an Hosting Provider environment (a "Transaction Link"). The DMZ at the Hosting Provider Data Centers is connected through VPN tunnels that terminate on the Hosting Provider firewalls. For all other Hosting Provider Data Centers, the HPISN DMZ connects to the Hosting Provider Data Center network via a direct link though a Firewall Interconnect Network (FIN).	Y		
H3	1	63	H3.1.63	Network	WAN	Hosting Provider configures the VPN device based on Customer's network topology and Hosting Provider policies. The Hosting Provider-provided VPN has two interfaces, external and internal. Hosting Provider generally uses both interfaces (dual-arm mode), but can support a configuration that uses only one interface (single-arm mode).	Y		
H3	1	64	H3.1.64	Network	WAN	The external interface should be connected to a switch between Customer's border router and firewall.	Y		
H3	1	65	H3.1.65	Network	WAN	The VPN device external interface may be connected to a firewall DMZ interface.	Y		
H3	1	66	H3.1.66	Network	WAN	The VPN Device external interface shall not be directly connected to the Internet. The external untrusted interface should be connected to the Internet behind Customer's boarder router to enable Customer to apply Access Control Lists (ACLs) to secure Customer's Environment from unsolicited traffic.	Y		
H3	1	67	H3.1.67	Network	General	Solutions will use TCP/IP as its networking protocol.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Backup Recovery

Base	Level	Sub	Req ID New	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence	Source
H4	1	1	H4.1.1	Backup Recovery	General	Backup and Recovery Services, retention and performance will be compliant with HIPAA, IRS 1075, PCI-DSS standards.	Y			Hosting, Backup, Recovery Hosting NFR 2012 draft v1 12172012 MKM
H4	1	2	H4.1.2	Backup Recovery	General	Backup Recovery Services will be in place for Production Environment and Non-Production Environments.	N (Yes for Production and Development)			
H4	1	3	H4.1.3	Backup Recovery	General	Backup and Recovery Services will include operating system images, configuration files, database, code tree, hardware configurations and virtualization configurations.	Y			Hosting, Backup, Recovery Hosting NFR 2012 draft v1 12172012 MKM
H4	1	4	H4.1.4	Backup Recovery	General	Backup Recovery Services will be in Place for Disaster Recovery Environment(s) and mirror Production Environments.	Y (backup is not active until a declaration to transition to the DR site for production operations, backup will be in place and operational)			Hosting, Backup, Recovery Hosting NFR 2012 draft v1 12172012 MKM
H4	1	5	H4.1.5	Backup Recovery	General	Full backups of Customers's Environments shall be written to disk daily and copied to tape twice a week; database and code tree backup tapes are retained at an off-site facility for eight weeks. Production Support Environment backups are copied to tape once a week and retained at an off-site facility for eight weeks.	N (Full weekly back up with daily incrementals with 7 year montly tapes off-site)			Hosting, Backup, Recovery Hosting NFR 2012 draft v1 12172012 MKM
H4	1	6	H4.1.6	Backup Recovery	General	Hosting Provider will perform and store one baseline backup of the database, application code tree, and archive logs, upon Customer's request and prior to achieving Production Ready Status. The baseline backup will be stored for a period of three months at an off-site facility.	N (discussion with M Morey supporting this requirment)			Hosting, Backup, Recovery Hosting NFR 2012 draft v1 12172012 MKM
H4	1	7	H4.1.7	Backup Recovery	Overall availability	Backup solutions shall support 99.9% application availability.	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	8	H4.1.8	Backup Recovery	Recovery point objective	The recovery point objective (RPO) shall be 30 minutes	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	9	H4.1.9	Backup Recovery	Recovery time objective	The recovery time objective (RTO) shall be four (4) hours	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	10	H4.1.10	Retention	Database Log retention	Solutions shall keep log files on disk for 1 week, archive (compress, to tape ,etc) and keep for a month and purge the archives if older than a month.	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	11	H4.1.11	Backup Recovery	Offsite backup storage	One copy of the backup should store at off-site location daily.	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	12	H4.1.12	Backup Recovery	Availability during backup	Backups should be completed while the application is still active and supporting users.	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	13	H4.1.13	Backup Recovery	Procedure definition and training	Procedures must be defined and adequate personnel trained to recover the system state from a consistent set of backup data.	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	14	H4.1.14	Backup Recovery	Backup and recovery procedures	Backup/Recovery procedures should be successfully executed multiple times prior to the production launch of the system to validate the procedures and affirm ability to meet recovery requirements.	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	15	H4.1.15	DR	DR testing	Every quarter DR facility should be tested for full recovery within 24 hour timeframe.	N (DR test will be annual)			Vermont HIX Non-Functional_Requirements V1.0
H4	1	16	H4.1.16	DR	DR topology	Disaster Recover facility and Environment will provide a mirror of Production Environment and can meet RPO and RTO requirements.	Y			Vermont HIX Non-Functional_Requirements V1.0
H4	1	17	H4.1.17	Backup Recovery	Contractor	The contractor shall store backed-up data apart from the production data center that are at least 60 miles or as agreed upon by the Contractor and the Exchange to prevent simultaneous loss of production and backup data stores.	Y			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Capacity and Performance Management

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H5	1	1	H5.1.1	Capacity / Performance Management		Hosting Provider will perform Capacity management which is the process of planning, analyzing, sizing, and optimizing capacity to enable the Production Environment to handle data processing demand in accordance with the contracted Hosting Provider Services ("Capacity Management").	Y		
H5	1	2	H5.1.2	Capacity / Performance Management		Hosting Provider will perform Capacity Management which is provided for both reactive and proactive capacity assessments. Reactive capacity assessments are conducted in response to an Incident in which capacity issues may have been a contributing cause. Proactive capacity assessments are conducted as part of the Periodic Maintenance Plan for the Production Environment as a preventive measure in an attempt to avoid the occurrence of a capacity-related Incident. Reactive and proactive capacity assessments leverage performance and utilization data from the Production Environment, along with the current Architecture Document to determine if utilization is at or is trending toward a capacity limit. If a capacity limit is identified from the capacity assessment, Hosting Provider may recommend an increase to capacity.	Y		
H5	1	3	H5.1.3	Capacity / Performance Management		Hosting Provider will collect performance and capacity metrics	Y		
H5	1	4	H5.1.4	Capacity / Performance Management		Hosting Provider will conduct analysis of capacity-related metrics in reaction to monitoring alerts or incidents that may indicate possible capacity issues	Y		
H5	1	5	H5.1.5	Capacity / Performance Management		Hosting Provider will conduct Capacity Management periodically as part of the Periodic Maintenance Plan	Y		
H5	1	6	H5.1.6	Capacity / Performance Management		Hosting Provider will periodically review storage requirements and alert Customer as capacity limits are approached	Y		
H5	1	7	H5.1.7	Capacity / Performance Management		Hosting Provider will make recommendations to Customer of appropriate configuration and/or architecture Changes to address identified capacity issues	Y		
H5	1	8	H5.1.8	Capacity / Performance Management		Hosting Provider will, when recommending Changes to Customer's architecture, create an updated architecture document that reflects such changes	Y		
H5	1	9	H5.1.9	Capacity / Performance Management		Hosting Provider will implement Changes to address capacity issues following review with Customer in accordance with the Release Management process	Y		
H5	1	10	H5.1.10	Capacity / Performance Management		Hosting Provider will modify workload to best utilize existing capacity if capacity issues are related to workload management (e.g., batch job scheduling, report execution, etc.)	Y		
H5	1	11	H5.1.11	Capacity / Performance Management		Hosting Provider will establish workload management practices to distribute the batch workload across the daily, weekly, and monthly production schedules, including scheduling of batch jobs, execution of reports, and all other business activity that impacts system performance	Y		
H5	1	12	H5.1.12	Capacity / Performance Management		Hosting Provider will ensure batch workload is distributed across all available and appropriate system resources	Y		
H5	1	13	H5.1.13	Capacity / Performance Management	Load Balancing	Hardware and Network should support load balancing technologies for high availability and maintenance	Y		
H5	1	14	H5.1.14	Capacity / Performance Management	Continuous scalability	Server workloads should scale on-demand without shutting down the application	Y		
H5	1	15	H5.1.15	Capacity / Performance Management	Storage scalability	Storage should be flexible enough to add additional capacity of disks with minimal service disruption	Y		
H5	1	16	H5.1.16	Capacity / Performance Management	Seasonable load scalability	Server capacity should support month end and year end processing capacity	Y		
H5	1	17	H5.1.17	Capacity / Performance Management	Peak Concurrent Internal Users	System should support 500 concurrent internal users at peak time (6:00am - 6:00pm EST).	N (estiamted 400 concurrent end users)		
H5	1	18	H5.1.18	Capacity / Performance Management	Off-peak Concurrent Internal Users	System should support 100 concurrent internal users during Off-Peak hours (6:00pm - 6:00am EST).	Y		
H5	1	19	H5.1.19	Capacity / Performance Management	Peak Concurrent External Users	System should support X concurrent external users at peak time (6:00am - 6:00pm EST).	Y (built in 400 concurrent users)		
H5	1	20	H5.1.20	Capacity / Performance Management	Off-peak Concurrent External Users	System should support X concurrent internal users during Off-Peak hours (6:00pm - 6:00am EST).	Y (built in 400 concurrent users)		
H5	1	21	H5.1.21	Capacity / Performance Management	Server CPU utilization	The server(s) CPU utilization is not to exceed 85%	Y		
H5	1	22	H5.1.22	Capacity / Performance Management	Server memory utilization	The server(s) memory utilization is not to exceed 90%	Y		
H5	1	23	H5.1.23	Capacity / Performance Management	Server storage utilization	The server(s) disk space utilization is not to exceed 80%	Y		
H5	1	24	H5.1.24	Capacity / Performance Management	LAN collision rate	The Local Area Network (LAN) collision rate is not to exceed 20%	Y		
H5	1	25	H5.1.25	Capacity / Performance Management	WAN utilization	The Wide Area Network (WAN) utilization is not to exceed 80%	Y		

H5	1	26	H5.1.26	Capacity / Performance Management	Storage growth	Storage should provision 20% growth of data per year	N (no growth planned)		
H5	1	27	H5.1.27	Capacity / Performance Management	Server network speed	Inter-server communication should be on a Gigabit-class network with appropriate switch support	Y		
H5	1	28	H5.1.28	Capacity / Performance Management	Switch standard clustered databases	Clustering of database servers and application should connect thru private network.	Y		
H5	1	29	H5.1.29	Capacity / Performance Management	Application Requirement	Solutions shall be designed for ease of maintenance and readily allow future functional enhancements.	Y		
H5	1	30	H5.1.30	Capacity / Performance Management	Application Requirement	Solutions shall be adequately flexible to keep up with ever changing technology and regulatory changes.	Y		
H5	1	31	H5.1.31	Capacity / Performance Management	Application Requirement	Solutions shall be scalable and adaptable to meet future growth and expansion needs such that Solutions can be expanded and be able to retain its performance levels when adding additional users, functions, and data.	Y		
H5	1	32	H5.1.32	Capacity / Performance Management	Application Requirement	The screens shall be highly re-configurable, providing ability to reposition and rename field labels, remove or turn-off unused fields, maintain data, and allow addition of custom-defined fields.	Y		
H5	1	33	H5.1.33	Capacity / Performance Management	Application Requirement	State shall be able to modify the labels and arrangement of information in the data model Solution documentation templates and can create custom data fields.	Y		
H5	1	34	H5.1.34	Capacity / Performance Management	Application Requirement	Solutions shall provide the ability to create and/or modify edits and business rules which determine the correctness/integrity of data.	Y		
H5	1	35	H5.1.35	Capacity / Performance Management	General	Solutions shall provide the ability for on-line access by any site connected to the organization Wide Area Network (WAN).	Y		
H5	1	36	H5.1.36	Capacity / Performance Management	Application Requirement	Solutions shall provide the capability for remote access in compliance with existing State connectivity/security policies	Y		
H5	1	37	H5.1.37	Capacity / Performance Management	Application Requirement	Solutions response time during peak agency level operations shall be 3 seconds or less for 95 percent of the search and lookup queries (does not include adhoc queries and analytics). Maximum response time shall not exceed 15 seconds except for agreed to exclusions. Response time is defined as the time elapsed after depressing an ENTER key (or clicking on a button that submits the screen for processing) until a response is received back on the same screen.	Y		
H5	1	38	H5.1.38	Capacity / Performance Management	Application Requirement	Solutions shall be built such that expansion of the system can be achieved with a minimum of additional system administration burden and staffing.	Y		
H5	1	39	H5.1.39	Capacity / Performance Management	Application Requirement	Solutions administration staffing requirements and workload should be minimally impacted with expanded system usage.	Y		
H5	1	40	H5.1.40	Capacity / Performance Management	Application Requirement	Solutions shall be built so that there is a near linear relationship between each additional server added, and the additional load that can be accommodated (load vs. capacity added), up to specified limit.	Y		
H5	1	41	H5.1.41	Capacity / Performance Management	A4.17	Solutions shall provide the ability to recover from data loss due to end user error and end application error.	Y		
H5	1	42	H5.1.42	Capacity / Performance Management	A4.18	Solutions shall provide the ability to perform archival/incremental backups and the ability to perform open/closed database backups.	Y		
H5	1	43	H5.1.43	Capacity / Performance Management	A4.19	Solutions shall provide tools included for managing an environment that supports both high availability and disaster recovery.	Y		
H5	1	44	H5.1.44	Capacity / Performance Management	A4.2	Solutions shall return a Dashboard report within 5 seconds or less from all user locations with a high speed network connection (greater than 768KB), 95% of the time.	Y (for average webpage response)		
H5	1	45	H5.1.45	Capacity / Performance Management	A4.23	Solutions shall include the capability to maintain all data according to state defined records retention guidelines (i.e. record schedule). General schedules can be found at: http://vermont-archives.org/records/schedules/general/. Specific retention disposition orders can be found at: http://Customer-archives.org/records/schedules/orders/. In general document retentions range from 3 to 10 years. In addition to the above note that case records including Child Support-related data must be retained for a minimum of 3 years after Case closure and the youngest child in the case is 18 years old.	Y		
H5	1	46	H5.1.46	Capacity / Performance Management	A4.25	Solutions shall provide on-line access of up to 6 months of data to be used for processing eligibility.	Y		
H5	1	47	H5.1.47	Capacity / Performance Management	A4.4	Solutions shall return a parameter-based report within 20 seconds or less.	Y (on average)		
H5	1	48	H5.1.48	Capacity / Performance Management	A4.5	Solutions will give the highest priority to Search and Look up operations performance, conforming to the minimum acceptable performance standard of 5 seconds response time, for 95% of queries.	Y (on average)		
H5	1	49	H5.1.49	Capacity / Performance Management	A4.6	Solutions shall be available for use 99.9% of the time (no more than 8.8 hours of downtime per year).	Y		
H5	1	50	H5.1.50	Capacity / Performance Management	A4.7	Solutions shall be architected with no single point of failure, supporting a high-availability enterprise	Y		
H5	1	51	H5.1.51	Capacity / Performance Management	A4.8	Hours of operations shall be 24 hours per day, 7 days per week, and 365 days a year.	Y		
H5	1	52	H5.1.52	Capacity / Performance Management	A4.9	Solutions shall have the ability to support session replication and transparent failover using high-availability processor architectural options.	Y		

H5	1	53	H5.1.53	Capacity / Performance Management	Failure Detection, Notification, and Restart	All components must be provided with a framework for automatic failure detection, notification, and restart.	Y		
H5	1	54	H5.1.54	Capacity / Performance Management	Remote Diagnostics	All servers must be capable of remote diagnosis,configuration, personalization, and other types of administration.	Y		
H5	1	55	H5.1.55	Capacity / Performance Management	Event Creation and Notification	The architecture must provide standardized services for general event creation and notification.	Y		
H5	1	56	H5.1.56	Capacity / Performance Management	First Failure Data Capture	First failure data capture means that sufficient error and diagnostic information is captured to allow problem source identification without recreating the problem.	Y		
H5	1	57	H5.1.57	Capacity / Performance Management	First Failure Data Capture	The architecture must provide standardized services for first failure data capture in error handling. All components of the architecture and application code must implement the concept of first failure data capture.	Y		
H5	1	58	H5.1.58	Capacity / Performance Management	Monitoring	It is the responsibility of the enterprise management framework to provide monitoring and alarm services for the environment.	Y		
H5	1	59	H5.1.59	Capacity / Performance Management	Monitoring detail	Monitoring tools must provide sufficient detail to identify the source and nature of faults.	Y		
H5	1	60	H5.1.60	Capacity / Performance Management	Monitoring communication	The tools should also support alert communication via email and text messages and automated response capability (e.g. An error event causes a script to be executed to restart a service).	Y		
H5	1	61	H5.1.61	Capacity / Performance Management	Enterprise management interoperability	The architecture must work closely with the enterprise management framework to provide the appropriate events.	Y		
H5	1	62	H5.1.62	Capacity / Performance Management	Transaction tracability	The architecture must provide the capability to track and review transactions through the system for the purposes of auditing, error diagnosis, and performance management. At a minimum this traceability should be at the component interface level. Ideally this should be implemented in a fashion that allows dynamic starting and stopping of this service.	Y		
H5	1	63	H5.1.63	Capacity / Performance Management	Transaction visibility	Using a combination of instrumentation within code and monitoring tools. It is expected that the environment will be managed through an overall quality process that includes the analysis of performance and availability results. The architecture needs to support the extraction and analysis of this information.	Y		
H5	1	64	H5.1.64	Capacity / Performance Management	Modular component modifiability	Ensuring the ability to apply changes at the component and data level. The goal is to be able to make these changes with no loss of availability at the application or component level.	Y		
H5	1	65	H5.1.65	Capacity / Performance Management	Monitor performance and utilization	The architecture must provide the ability to record and monitor the performance and utilization of resources within the overall system and individual component types	Y		
H5	1	66	H5.1.66	Capacity / Performance Management	Technology component monitoring	Individual technology components (e.g., SOA, MDM, IdM) shall be monitored using an enterprise monitoring tool.	Y		
H5	1	67	H5.1.67	Capacity / Performance Management	Component level monitoring	The system must measure and record performance metrics at a system component level so that appropriate reports can be generated for monitoring purposes.	Y		
H5	1	68	H5.1.68	Capacity / Performance Management	UI Response Time	UI level transaction should complete in 5 seconds	Y (on average)		
H5	1	69	H5.1.69	Capacity / Performance Management	Query Response Time	Query thru UI layer should show results in 15 seconds	Y (on average)		
H5	1	70	H5.1.70	Capacity / Performance Management	Data Refresh	Datawarehouse and other non-OLTP data sources shall be refreshed within 24 hours	Y (on average)		
H5	1	71	H5.1.71	Capacity / Performance Management	non-functional	Project teams (vendor-supplied or otherwise) shall develop a Capacity Plan to include, at minimum, the following areas: - A description of how the solution's capacity and capacity requirements were calculated, including all formulas and calculations used in capacity planning for the State. - A description of how the solution's capacity requirements will be met. - How capacity issues will be managed for all components of the State project. - Descriptions of how capacity utilization will be monitored and capacity thresholds will be established. - A description of corrective and escalation processes that will be used in the event any capacity thresholds are reached.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Configuration Management

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H6	1	1	H6.1.1	Configuration Management		Hosting Provider will maintain Configuration Management which is the process of identifying, recording, and reporting of Infrastructure components (hardware, software, and associated documentation), including their versions, constituent components, and relationships.	Y		
H6	1	2	H6.1.2	Configuration Management		Hosting Provider will maintain an Architecture Document to represent the current configuration of the Environment	Y		
H6	1	3	H6.1.3	Configuration Management		Hosting Provider will account for all IT assets and configurations within the Environment	Y		
H6	1	4	H6.1.4	Configuration Management		Hosting Provider will conduct audits as necessary to validate the physical existence of configuration components and accuracy of configuration management data	Y		
H6	1	5	H6.1.5	Configuration Management		Hosting Provider will maintain accurate documentation on configurations to support other service management processes	Y		
H6	1	6	H6.1.6	Configuration Management		Hosting Provider will maintain configuration records of changes to Third Party Software	Y		
H6	1	7	H6.1.7	Configuration Management		Hosting Provider will assume responsibility for configuring, managing and tracking all equipment and software at Vermont's locations that is considered part of Hosting Providers Programs.	Y		
H6	1	8	H6.1.8	Configuration Management		Project teams (vendor-supplied or otherwise) shall submit to the State as part of their proposal, specifications for all necessary hardware, software and tools for the six (6) target environments listed here. Project teams can propose to combine certain environments, where appropriate. The six (6) environments include: 1. Production 2. Staging 3. Development 4. Test 5. Training 6. Disaster Recovery. Project teams shall submit as a component of proposal specifications for all software, hardware, and tools that would be inclusive of a full SDLC.	Y		
H6	1	9	H6.1.9	Configuration Management		Project teams (vendor-supplied or otherwise) shall develop a technical infrastructure document which describes all of the hardware, system software and tools necessary for each proposed deployment environment.	Y		
H6	1	10	H6.1.10	Configuration Management		Project teams (vendor-supplied or otherwise) shall develop an environment configuration manual that describes the environment installation and configuration necessary deployent environment.	Y		
H6	1	11	H6.1.11	Configuration Management		Project teams (vendor-supplied or otherwise) are responsible for installing, configuring, and maintaining all hardware, software and tools purchased under any contract until solution acceptance for the proposed deployment environments.	Y		
H6	1	12	H6.1.12	Configuration Management		Project teams (vendor-supplied or otherwise) shall provide the State with readable source code and object (executable) code, documentation for all functionality developed by Project teams (vendor-supplied or otherwise), licenses to readable source code and object (executable) code, and documentation for all COTS functionality and escrow of source code for the COTS. All new software functionality built on top of COTS software shall be owned by the State.	Y		
H6	1	13	H6.1.13	Configuration Management		Project teams (vendor-supplied or otherwise) shall provide a data dictionary and data model for the State.	Y		
H6	1	14	H6.1.14	Configuration Management		The Hosting Provider shall provide exit plan addressing portability of solution in case Customer wants to transition Environment to another Hosting Provider. (See Transition Requirements)	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Release Management

Base	Level	Sub	Req ID New	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H7	1	1	H7.1.1	Release Management		Hosting Provider shall have a standard Maintenance Windows for purposes of applying Infrastructure Releases. These Maintenance Windows differ from the time frame set between Hosting Provider and Customer for Customer-specific Release Management activities.	Y		
H7	1	2	H7.1.2	Release Management		Hosting Provider will provide notification when it intends to use standard Maintenance Windows in lieu of another time frame scheduled for Customer-specfiic Release Management activities.	Y		
H7	1	3	H7.1.3	Release Management		Hosting Provider will perform maintenance on Infrastructure during a three-hour Weekly Maintenance Window that will not effect solution availability	Y		
H7	1	4	H7.1.4	Release Management		Hosting Provider will as deemed necessary by Hosting Provider, but no more than twice per year, perform maintenance on Customer's Infrastructure during a 12-hour window (the "Semiannual Maintenance Window")	Y		
H7	1	5	H7.1.5	Release Management		Component changes may include but are not limited to hardware replacement, operating system patches and upgrades, and configuration changes.	Y		
H7	1	6	H7.1.6	Release Management		Infrastructure Components may include but are not limited to Servers, network devices, and storage.	Y		
H7	1	7	H7.1.7	Release Management		Hosting Provider will send email notifications, including an overview of the Release, within minimum 72 hours in advance of use of a Weekly Maintenance Window and 30 days in advance of use of a Semiannual Maintenance Window	Y		
H7	1	8	H7.1.8	Release Management		Hosting Provider will use commercially reasonable efforts to coordinate the timing of Release-related maintenance activities	Y		
H7	1	9	H7.1.9	Release Management		Hosting Provider will have approval for Changes to Infrastructure components requested by Hosting Provider that will be implemented outside the standard Maintenance Windows and will affect functionality	Y		
H7	1	10	H7.1.10	Release Management		When functionality is ready to be delivered to the Customer for User Acceptance Testing (UAT), it shall be delivered in the form of a pre-production release. Since the Customer will approve all releases into production, a pre-production release is equivalent to a production release and requires the rigor associated with a production release. Upon successful completion of UAT, the Customer will schedule a release to be moved to the production environment. Each pre-production release shall include the following: - Release-specific hardware and software Solution components. - Release description including architecture or design updates, new functionality introduced, defects fixed, modifications to interfaces with other systems, other changes to existing code, and any software and hardware configuration changes. - Release contents including a description of the release structure and contents and instructions for assembling and/or configuring the components of the release. - Test Plan and test execution results. - Detailed hardware and software configuration information including any software and hardware dependencies and instructions at a level of detail that will enable administrators staff to rebuild and configure the hardware environment without outside assistance. - Database documentation conforming to industry standards. - Detailed configuration information for any 3rd party hardware and software. Project teams (vendor-supplied or otherwise) shall provide updated documentation when upgrades to software or equipment occurs through the life of the contract or project.	Y		
H7	1	11	H7.1.11	Release Management		Upon successful completion of the pre-production testing, Project teams (vendor-supplied or otherwise) shall, in coordination with the Customer, create a Production Release Plan that shall consist of an updated Pre-Production Release notification to assist the Customer in successfully releasing and maintaining the Solution in the Production environment. It must include, but not be limited to, the following components: - Updated Configuration Information required satisfying the solutions' production configuration management requirements. - Updated Solution Architecture. - Updated Detailed Design, including detailed system, technical, and user documentation. - Deployment schedule	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Monitoring Management

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H8	1	1	H8.1.1	Monitoring		Hosting Provider will install Hosting Provider Tools on Servers within Vermont's Infrastructure that enable monitoring and management capabilities	Y		
H8	1	2	H8.1.2	Monitoring		Hosting Provider will identify event threshold violations for proactive response	Y		
H8	1	3	H8.1.3	Monitoring		Hosting Provider will facilitate configuration of monitoring events	Y		
H8	1	4	H8.1.4	Monitoring		Hosting Provider will provide performance management historical data, such as operating system performance graphs upon request and where such data is available	Y		
H8	1	5	H8.1.5	Monitoring		Hosting Provider will provide network performance monitoring, including WAN/LAN link utilization, latency and loss, and key LAN switch port performance monitoring	Y		
H8	1	6	H8.1.6	Monitoring		Hosting Provider will report Outages and Service Interruptions when identified	Y		
H8	1	7	H8.1.7	Monitoring		Hosting Provider will monitor the network on the Vermont side and the WAN link from Vermont to Hosting Provider	Y		
H8	1	8	H8.1.8	Monitoring		As part of Monitoring Services, Hosting Provider will use information collected by the Tools to monitor use, performance and availability of the Hosting Provider Programs and Computer and Administration Services and to help resolve service requests.	Y		
H8	1	9	H8.1.9	Monitoring		Hosting Provider will monitor the services by utilizing a variety of Tools at various layers in the Technology Stack of the Environment ("Monitoring Services"). The Hosting Provider monitoring Tools are designed to collect, compile, and provide information about the capacity, performance, availability, and configuration of the Hosting Provider Programs running in the Environment, and about the configurations and the operational state of hardware, operating systems, and Hosting Provider services system support.	Y		
H8	1	10	H8.1.10	Monitoring	transaction monitoring and logging	Solutions shall detect major errors related to one or more components including loss of network connectivity, a database server going off line, or the application suffers a out-of-memory situation	Y		
H8	1	11	H8.1.11	Monitoring	transaction monitoring and logging	Solutions shall allow for different roles for Users including Operators, Administrators, Managers etc	Y		
H8	1	12	H8.1.12	Monitoring	transaction monitoring and logging	Solutions shall allow for Report generation and analysis for application troubleshooting and capacity planning.	Y		
H8	1	13	H8.1.13	Monitoring	transaction monitoring and logging	The State of Vermont and AHS have not identified a preference for a performance management toolset. Project teams (vendor-supplied or otherwise) should propose one or more monitoring tool(s) to proactively monitor the performance of key infrastructure components of the proposed System.	Y (CGI standard tool sets)		
H8	1	14	H8.1.14	Monitoring	transaction monitoring and logging	Solutions shall detect less than desirable application performance, such as degraded servlet, database or other back end resource response times.	Y		
H8	1	15	H8.1.15	Monitoring	transaction monitoring and logging	Solutions shall have safeguards designed to ensure that configuration variables affecting the application and the back end resources remain at some predetermined configuration settings.	Y		
H8	1	16	H8.1.16	Monitoring	transaction monitoring and logging	Solutions shall detect intrusion attempts by unauthorized system users.	Y		
H8	1	17	H8.1.17	Monitoring	transaction monitoring and logging	Solutions shall monitor critical performance parameters such as response time, resource availability, CPU Utilization, etc.	Y		
H8	1	18	H8.1.18	Monitoring	transaction monitoring and logging	Solutions shall provide a holistic view of a wide range of application services and network services	Y		
H8	1	19	H8.1.19	Monitoring	transaction monitoring and logging	Solutions shall send alarms based on the monitored attributes. These can be escalated through E-Mail / SMS etc.	Y		
H8	1	20	H8.1.20	Monitoring		Solutions shall allow to perform admin activities through an intuitive user interface. Shall have the ability to create custom dashboards to empower the users.	Y		
H8	1	21	H8.1.21			Hosting Provider shall utilize a network-based monitoring approach to detect attacks on open firewalls ports.	Y		
H8	1	22	H8.1.22			Network intrusion events are analyzed using signature detection against a database of known attacks which is updated as soon as new releases become available.	Y		
H8	1	23	H8.1.23			Network instrusion alerts are forwarded to Hosting Providers IT security and Service Desk immediately for review and response.	Y		
H8	1	24	H8.1.24			Hosting provider shall employ a separate extranet for hosting servers separating them from its internal corporate network.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Service Continuity Management

Base	Level	Sub	Req ID/New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H9	1	1	H9.1.1	Service Continuity Management		Hosting Provider will provide Service Continuity Management for the Production Environment following a declared Disaster.	Y		
H9	1	2	H9.1.2	Service Continuity Management		Disaster declaration will occur no later than 24 hours of Customers Application service becoming unavailable and will be a shared decision between Customer and Hosting Provider.	Y		
H9	1	3	H9.1.3	Service Continuity Management		Customer may install the data and files from the applicable backup delivered by Hosting Provider onto a system(s) provided by Customer either at its facility or at a third party facility that it designates.	Y (assuming proper security and regulatory needs are supported)		
H9	1	4	H9.1.4	Service Continuity Management		Hosting Provider will conduct regular system backups of the Environment(s) following the frequency and retention outlined by Customer.	Y		
H9	1	5	H9.1.5	Service Continuity Management		In the event of a Disaster, within seven days from the time when a Disaster is declared, deliver to Customer's address and contact person specified a backup containing the database, code tree and archive logs that resided on the Production Environment at the time that Hosting Provider created such backup.	Y		
H9	1	6	H9.1.6	Service Continuity Management		Hosting Provider will use reasonable efforts to restore access to and use of the Production Environment (including the recovery of production data) located at Hosting Provider's Data Center following declaration of the Disaster.	Y		
H9	1	7	H9.1.7	Service Continuity Management		If determined that deployment at a Customer-retained secondary site (DR) is required for restoration and use of the Production Environment, use reasonable efforts to provide Customer with information that Customer reasonably requires to select DR cutover.	Y		
H9	1	8	H9.1.8	Service Continuity Management		Hosting Provider will ship to the Customer address and contact person specified a data export that consists of data from Customer's Production database upon request.	Y		
H9	1	9	H9.1.9	Service Continuity Management		Solutions (Application Services) shall be restored in less than 4 hours (RTO), and only experience the loss of the 30 minutes (RPO) of transactions.	Y		
H9	1	10	H9.1.10	Service Continuity Management		Solutions shall support a Production and hot (real time replication) DR design that would allow one site to seamlessly be offline and the other site would maintain service without interruption meeting RPO and RTO requirements.	Y		
H9	1	11	H9.1.11	Service Continuity Management		Solutions shall include a disaster recovery plan and provide contingency plans to Customer for application services managed by Hosting Provider.	Y		
H11	1	12	H11.1.12	Service Continuity Management		Solutions shall have business continuity plans	Y (for DR plan)		
H11	1	13	H11.1.13	Service Continuity Management		Solutions will maintain and effectively implement plans for emergency response, backup operations and post disaster recovery	Y		
H11	1	14	H11.1.14	Service Continuity Management		Disaster recovery requirements relative to the physical solution components and planning for recovery from operational failures are the responsibility of Project teams (vendor-supplied or otherwise) . Project teams (vendor-supplied or otherwise) shall develop an Operational Recovery Plan that addresses the following: - Areas of the solution most susceptible to failure or disaster that would result in downtime. - Recommendations for solution recovery processes, or steps to take in the event of a downtime event. - Recommendations for the State on how to comprehensively and effectively mitigate the risk of a downtime event. - Recommendations for securing the solution components during a period of emergency operation.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Refreshes and Lifecycle

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H10	1	1	H10.1.1	Refreshes and Lifecycle		Refresh Services shall be delivered by Hosting Provider and designed to be delivered 24 hours a day, 7 days a week, 365 days a year (excluding agreed to Maintenance Windows and Planned Outages).	Y		
H10	1	2	H10.1.2	Refreshes and Lifecycle		For each Environment set (consisting of a single Production Environment, Production Support Environment and Non-Production Environment(s)), Hosting Provider will perform all required number of Refreshes. Refreshes can be ondemand or scheduled based on Environment (Training versus Development). Hosting Provider-initiated Refreshes, such as Refreshes required as part of a data fix or Customer's Periodic Maintenance Plan will be approved by Customer.	Y		
H10	1	3	H10.1.3	Refreshes and Lifecycle		Refresh from Customer's existing Production Environment, Production Support Environment, and/or Non-Production Environment to a new environment, Hosting Provider will use as the new environment either (i) one of Customer's existing available Hosting Provider environments for which Hosting Provider is providing Computer and Administration Services or Administration Services, or (ii) a new Additional Non-Production Environment.	Y		
H10	1	4	H10.1.4	Refreshes and Lifecycle		Hosting Provider shall be able to reload an image copy of database files and application files from a backup to the Environment from which the copy was made (a "Restore").	Y		
H10	1	5	H10.1.5	Refreshes and Lifecycle		A Source Environment shall be defined as the Production Environment, Production Support Environment or Non-Production Environment from which the data for the Refresh will be obtained. The Target Environment is the Production Support Environment or Non-Production Environment to which the data for the Refresh will be applied.	Y		
H10	1	6	H10.1.6	Refreshes and Lifecycle		Database Refreshes shall consist of copying the database from the Source Environment to the Target Environment and making the required configuration Changes within the database of the Target Environment.	Y		
H10	1	7	H10.1.7	Refreshes and Lifecycle		Partial Refreshes shall consist of copying of the database and/or part of the application code from the Source Environment to the Target Environment and making the required configuration Changes within the database and application of the Target Environment.	Y		
H10	1	8	H10.1.8	Refreshes and Lifecycle		Full Refreshes shall consist of copying the database and full application code from the Source Environment to the Target Environment and making the required configuration changes within the database and application of the Target Environment.	Y		
H10	1	9	H10.1.9	Refreshes and Lifecycle		Code Refreshes consist of copying full application code from the Source Environment to the Target Environment and making the required configuration Changes within the application tier of the Target Environment.	Y		
H10	1	10	H10.1.10	Refreshes and Lifecycle		Configuration Migration shall consist of copying application metadata and artifacts from the Source Environment to the Target Environment and making the required configuration Changes within the Target Environment.	Y		
H10	1	11	H10.1.11	Refreshes and Lifecycle		Hosting provider will develop with Customer a Refresh Schedule to perform the Refreshes identified.	Y		
H10	1	12	H10.1.12	Refreshes and Lifecycle		Hosting provider will perform the Refreshes identified in the using a backup of the Source Environment.	Y		
H10	1	13	H10.1.13	Refreshes and Lifecycle		Hosting provider will perform Refreshes in accordance with standard Hosting Provider procedures and guidelines.	Y		
H10	1	14	H10.1.14	Refreshes and Lifecycle		Hosting provider will perform Refreshes based on a submitted and approved change request from Customer	Y		
H10	1	15	H10.1.15	Refreshes and Lifecycle		No more than one Refresh per Production Environment may be executed at a single point in time or otherwise run simultaneously.	Y		
H10	1	16	H10.1.16	Refreshes and Lifecycle		Hosting provider shall work with one contact at Customer for coordination of refreshes	Y		
H10	1	17	H10.1.17	Refreshes and Lifecycle		Refreshes shall be provided more frequently during the implementation phase as compared to the Post Production Go-Live phase.	Y		
H7	1	18	H7.1.18	Release Managen		Database Data exports can contain all data from Customer's Production database(s).	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Maintenance and Operations

Base	Level	Sub	ReqID New	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H11	1	1	H11.1.1	Maintenance and Operations	Contractor	Hosting provider shall conduct testing on any changes,upgrades to hardware or patches applied to ensure backward compatibility of its solution and integration within Customer's Environments	Y		
H11	1	2	H11.1.2	Maintenance and Operations	Contractor	The contractor shall work with the Customer in advance of any release or changes to allow the Exchange team to adequately test, verify and train to support the smooth operation of the Customers Applications and its solutions	Y		
H11	1	3	H11.1.3	Maintenance and Operations	Contractor	Hosting provider shall provide access for appropriate and authorized Customer team members to the test and training environments to ensure correct implementation of changes before the changes are released to the production environment	Y		
H11	1	4	H11.1.4	Maintenance and Operations	Contractor	Hosting provider shall provide version control management capability. All changes to the solution shall be reported and approved by the state, be maintained in the Contractor's version control management solution, which shall be available to the Customer for review and audit as needed.	Y		
H11	1	5	H11.1.5	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall describe the production support and transition approach and methodology used for solutions.	Y		
H11	1	6	H11.1.6	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall establish an automated maintenance routine that shall at a minimum: - backup the user IDs and password data - identify expired IDs and related data	Y		
H11	1	7	H11.1.7	Maintenance and Operations	non-functional	Upon completion of any maintenance call, Project teams (vendor-supplied or otherwise) shall furnish a maintenance activity report to the State within 24 hours, which shall include, at minimum, the following: - Date and time notified. - Date and time of arrival. - If hardware, type and serial number(s) of machine(s). - If software, the module or component name of the affected software code. - Time spent for repair. - List of parts replaced and/or actions taken. - Description of malfunction or defect.	Y		
H11	1	8	H11.1.8	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall produce the solution's Operation Manual, which will serve as an operator's instruction manual. It will include solution administration procedures and describe the scheduled operations of the production system. It will contain specific instructions on things an operator needs to do to manage the solution on a daily basis, descriptions of administrative tasks, instructions on how to run the job, and what to do in abnormal situations.	Y		
H11	1	9	H11.1.9	Maintenance and Operations	non-functional	The solution component documentation shall include at a minimum: - A Data Dictionary - Data Model(s) - Interface design specifications - Passwords & activation codes - A Developer's Manual outlining and detailing operating, maintenance, development, processes, standards, procedures, plus any other technical information required to fully support the application. - Operations cycles and procedures including batch or background process schedule, dependencies, sequencing, and timing. - Administrative Tasks including users administration, solution security administration, reference data maintenance, creation of report templates and maintenance of service provider data and contracts. - Other reference materials and presentations required to supplement the training and support activities.	Y		
H11	1	10	H11.1.10	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall develop a High Availability & Disaster Recovery Plan for the entire solution based on the assumption that the solution's data will be recovered at an alternate data center as designated by the State.	Y		
H11	1	11	H11.1.11	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall provide documentation that describes the procedures for Solution administrators to add, update or remove user IDs and passwords.	Y		
H11	1	12	H11.1.12	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall submit a Help Desk Support Plan for use by the responsible entity help desk addressing: - Overview of support strategy assuming that the State will provide tier 1 and 2 help desk support - Help desk design - Help desk operations (processes and procedures) - Incident management procedures and processes including escalation - Problem management procedures and processes - Reporting	Y		
H11	1	13	H11.1.13	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall provide the responsible entity with help desk scripts and decision trees for tier 1 and 2 help desk support.	Y		
H11	1	14	H11.1.14	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall provide a Transition-Out Plan six months prior to production support contract expiration. The Plan must contain transition task descriptions, an organization chart, and job descriptions for all support staff.	Y		
H11	1	15	H11.1.15	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall provide instructions and training for responsible agency support staff that may need to access and support the solution remotely.	Y		
H11	1	16	H11.1.16	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall incorporate the production support and transition approach into a comprehensive Production Support and Transition Plan complying with the solution architectural design, that will describe how Project teams (vendor-supplied or otherwise) intends to support the solution and transition that support over to the entity responsible for on-going production operations and support.	Y		
H11	1	17	H11.1.17	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall agree to continue normal operations activities until completion of Transition-Out Plan activities.	Y		
H11	1	18	H11.1.18	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall, at a minimum, provide routine solution upgrades and fixes to the solution components at no additional cost. In addition, Project teams (vendor-supplied or otherwise) shall provide at no additional charge, routine solution upgrades and fixes to application software and field/technical services bulletins periodically as they become available within 24 hours after they receive them from application licensors, subOfferors, manufacturers, and other third parties.	Y		
H11	1	19	H11.1.19	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall provide the State with a list of personnel, contact information, and their area of expertise of who shall be performing solution production support.	Y		

H11	1	20	H11.1.20	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall repair any corrupted data that is associated with a problem in the solution.	Y		
H11	1	21	H11.1.21	Maintenance and Operations	non-functional	With concurrence from the State, the routine planned maintenance activities shall be scheduled without disrupting the negotiated operational hours. Offeror shall provide the State with a copy of the schedule at least 30 days in advance of the scheduled maintenance date for approval.	Y		
H11	1	22	H11.1.22	Maintenance and Operations	non-functional	The testing tools and test configurations shall be provided to the State and responsible entities as the solution is transitioned into support.	Y		
H11	1	23	H11.1.23	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall provide instructions and training for responsible entity support staff that may need to access and support the solution remotely (e.g. through PDAs, tablet PC's through a VPN).	Y		
H11	1	24	H11.1.24	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall develop an automated process for purging production solution files when necessary.	Y		
H11	1	25	H11.1.25	Maintenance and Operations	non-functional	Solutions shall be compatible with and protected/monitored at the network, systems and application level with the State's shared enterprise management components	Y		
H11	1	26	H11.1.26	Maintenance and Operations	non-functional	Application logs and error messages shall be monitored by the appropriate parties.	Y		
H11	1	27	H11.1.27	Maintenance and Operations	non-functional	Web-based solutions shall permit analysis of web logs	Y		
H11	1	28	H11.1.28	Maintenance and Operations	non-functional	The Exchange will ensure that new development on the system does not impact the production environment	Y		
H11	1	29	H11.1.29	Maintenance and Operations	non-functional	Solutions shall have critical security patches applied within 24 hours	Y		
H11	1	30	H11.1.30	Maintenance and Operations	non-functional	Solutions will ensure the system includes supported releases of all software, including any third part application components	Y		
H11	1	31	H11.1.31	Maintenance and Operations	non-functional	Solutions will include a supported release of all software.	Y		
H11	1	32	H11.1.32	Maintenance and Operations	non-functional	Solutions will support automated patch deployment.	Y		
H11	1	33	H11.1.33	Maintenance and Operations	Contractor	The hosting provider shall provide initial and ongoing maintenance and operations training for Customer staff.	Y		
H11	1	34	H11.1.34	Maintenance and Operations	non-functional	During the maintenance period, the maximum time to restore the functionality of applications and resolve incidents shall be within the timeframes listed in the Service Level Agreement. Incident Severity Level Definitions. ' Severity Level One incidents shall not exceed four (4) clock hours between the opening of an incident and final closure, unless a time extension is approved by the State. ' Severity Level Two incidents shall not exceed eight (8) business hours between the opening of an incident and final closure, unless a time extension is approved by the State. ' Severity Level Three incidents shall not exceed twenty four (24) business hours between the opening of an incident and final closure, unless a time extension is approved by the State. ' Severity Level Four incidents shall not exceed forty (40) business hours between the opening of an incident and final closure, unless a time extension is approved by the State.	Y		
H11	1	35	H11.1.35	Maintenance and Operations	non-functional	To prepare the State for a transition to another Infrastructure Service Provider, the Hosting Provider and Customer will collaboratively integrate the M&O Plan into the Customer's M&O Plan. The Hosting Provider shall develop a formal methodology to be used by the Customer and its new hosting provider to manage and operate the Solution during M&O that is documented in the Customers M&O Plan(s). The M&O Plan shall incorporate methodologies and practices which will assist the Customer and its new hosting vendor in successfully managing the's M&O life cycle and shall address at least the following areas: * Support Model * Triage Procedures * Tools * Identification of Roles and Responsibilities of support personnel * Release Management * Upgrades * Maintenance * On-going Operations * Customer Support * Specific support procedures for production * Deliverables - Requirement Traceability Matrix, Architecture and design, test procedure, case, and scripts * Resource Requirements (staff loading) * Capacity Management * Technology Refresh * Solution Security * Backup and Recovery * Disaster Recovery	Y		
H11	1	36	H11.1.36	Maintenance and Operations	non-functional	Solutions shall provide data archiving capabilities based on State defined criteria.	Y		

H11	1	37	H11.1.37	Maintenance and Operations	non-functional	All Solution communications shall be protected by at least 128-bit encryption.	Y		
H11	1	38	H11.1.38	Maintenance and Operations	non-functional	Solutions shall be supported by public key/private key encryption Secure Socket Layer (SSL) certificates.	Y		
H11	1	39	H11.1.39	Maintenance and Operations	non-functional	Solutions shall provide admin tools and maintenance routines to change access rights quickly.	Y		
H11	1	40	H11.1.40	Maintenance and Operations	non-functional	Solutions shall use firewalls and Demilitarized Zone (DMZ) for external access and remote access.	Y		
H11	1	41	H11.1.41	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to create and manage user accounts.	Y		
H11	1	42	H11.1.42	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign status and permissions to user accounts.	Y		
H11	1	43	H11.1.43	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to create and manage user roles.	Y		
H11	1	44	H11.1.44	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to create user groups to manage workflow.	Y		
H11	1	45	H11.1.45	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign users to particular local offices.	Y		
H11	1	46	H11.1.46	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign users to particular user groups / units.	Y		
H11	1	47	H11.1.47	Maintenance and Operations	non-functional	Solutions shall provide the capability to move all unnecessary data to offline storage according to a set of business rules and schedule to be defined by the State as a part of the ongoing system operational decision making.	Y		
H11	1	48	H11.1.48	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign users to particular supervisors.	Y		
H11	1	49	H11.1.49	Maintenance and Operations	non-functional	Solutions shall maintain an archival process so that accumulated historical records and log files do not consume large amounts of disk space.	Y		
H11	1	50	H11.1.50	Maintenance and Operations	non-functional	Solutions shall provide an auto archive/purge of the log files to prevent uncontrolled growth of the log and historical records storage using administrator-set parameters.	Y		
H11	1	51	H11.1.51	Maintenance and Operations	non-functional	Solutions shall provide version control capabilities to ensure the integrity of all software releases.	Y		
H11	1	52	H11.1.52	Maintenance and Operations	non-functional	Solutions shall provide logging, reporting for accessing errors and exceptions.	Y		
H11	1	53	H11.1.53	Maintenance and Operations	non-functional	Solutions shall monitor and provide reports on any unauthorized access.	Y		
H11	1	54	H11.1.54	Maintenance and Operations	non-functional	Solutions shall track unusual or out of normal Solution operations usage or user access.	Y		
H11	1	55	H11.1.55	Maintenance and Operations	non-functional	Solutions shall have the ability to generate administrative alerts and warnings when statistics indicate an impact or potential limits on solution component performance and availability. The specific alerts will be defined by the hosting services provider.	Y		
H11	1	56	H11.1.56	Maintenance and Operations	non-functional	Solutions shall allow for all changes/updates to the distributed components to be administered and completed centrally and available immediately to all source systems and sites.	Y		
H11	1	57	H11.1.57	Maintenance and Operations	non-functional	Solutions shall provide event management and monitoring functionality according to Information Technology Infrastructure Library version 3 (ITIL v3) or equivalent best practices.	Y		
H11	1	58	H11.1.58	Maintenance and Operations	non-functional	Solutions shall provide Application Performance Monitoring and Management capabilities (i.e. transaction monitoring, synthetic transactions, component root cause analysis (e.g. Application Server Management)	Y		
H11	1	59	H11.1.59	Maintenance and Operations	non-functional	Solutions shall provide transaction tracking and log consolidation capabilities across all tiers of the application	Y		
H11	1	60	H11.1.60	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall describe the implementation approach and methodology used for projects.	Y		
H11	1	61	H11.1.61	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall develop a Software Configuration Management Plan.	Y		
H11	1	62	H11.1.62	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall provide a software configuration management Solution to store, control, and track instances (baselines during the construction lifecycle) of all software configuration items developed for solutions.	Y		
H11	1	63	H11.1.63	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) must use an industry standard software configuration management tool.	Y		
H11	1	64	H11.1.64	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall describe the requirements management approach and methodology used for any proposed solution.	Y		

H11	1	65	H11.1.65	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall incorporate the requirements management approach into a comprehensive Requirements Management Plan. The Requirements Management Plan will be used by the project to assure that requirements are met. The Requirements Management Plan shall, at a minimum, address the following areas: - Establishment of a baseline for existing requirements. - Management of versions of requirements. - Establish and maintain the State's requirements traceability matrix that will be used for requirements management, and will map where in the software a given requirement is implemented. - A requirements change control process. - A methodology for managing requirements in an iterative development lifecycle. - Procurement, installation, and administration of requirements management tools. - A description of the relationship between the requirements management role and the other roles (i.e. test management, quality assurance management) on the project. - Publishing of standard reports related to requirements management.	Y		
H11	1	66	H11.1.66	Maintenance and Operations	non-functional	Deployment is expected to be iterative from both a business process and applied technology perspective. The State will accept the products into the production environment through application of the acceptance criteria in testing plans.	Y		
H11	1	67	H11.1.67	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall deliver to the State a requirements traceability matrix for all delivered functionality, showing all testing activities tracing to delivered functionality, and all delivered functionality tracing to requirements in the requirements repository.	Y		
H11	1	68	H11.1.68	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall assist the State with testing and release preparation in the pre-production environment.	Y		
H11	1	69	H11.1.69	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) must produce and execute an On-Site Implementation Support Plan.	Y		
H11	1	70	H11.1.70	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall incorporate the implementation approach into a comprehensive Implementation Plan. The State requires incremental deliveries of functionality to the production environment. The State anticipates considerable collaboration with Project teams (vendor-supplied or otherwise) in the plan's construction, with particular attention to high complexity components of the existing the State systems as well as the proposed solution.	Y		
H11	1	71	H11.1.71	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) must provide staff at the proposed number, ratios and duration for on-site support (as identified in previously submitted implementation approach and plan).	Y		
H11	1	72	H11.1.72	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) must assess the pre-implementation readiness of each part of the organization and shall document the status in a pre-implementation readiness assessment. Project teams (vendor-supplied or otherwise) shall conduct an implementation readiness review ten days prior to cutover at each part of the organization.	Y		
H11	1	73	H11.1.73	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall describe the approach to pilot the solution, including a high-level draft Pilot Plan.	Y		
H11	1	74	H11.1.74	Maintenance and Operations	non-functional	The Pilot Plan shall address at a minimum: - Pilot locations, users, durations, sequencing and timing - Pilot support model including roles and responsibilities of Project teams (vendor-supplied or otherwise) and the State; number of staff on-site and off-site; and staffing hours - How the pilot will be representative of staff from each broad category of work reflected in the State and represent the diversity in size of the various offices - Strategy for testing of all production functionality of the solution's components including interfaces to external systems - Reporting in the dual environment - Training of users and technical staff - Help desk procedures, functionality and incident reporting - Problem management procedures - Help related documentation - Functionality and operations of interfaces - Approach for validating worker productivity and efficiency - Approach for testing and validating mobility - Readiness planning - Plan and approach for resolving data corruption issues as a result of conversion - Change management processes - Approach for communication and coordination of pilot activities and issues - Approach and procedures for evaluating user experience and feedback - Approach and process for evaluation of the pilot against defined pilot success criteria - Detail process to validate the implementation process and tools and certify the State application, technical environment, and users as ready to move to full production implementation - Roll-back plan	Y		
H11	1	75	H11.1.75	Maintenance and Operations	non-functional	The pilot(s) shall test all solution components including at a minimum: - Training - Help desk - Production Support - Documentation - Interfaces - All Functionality - Reporting - Security - Problem escalation - Change process	Y		
H11	1	76	H11.1.76	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall produce a lessons learned document after conducting the Solution component pilots and provide recommendations for changes to the implementation process.	Y		
H11	1	77	H11.1.77	Maintenance and Operations	non-functional	The Implementation Plan must include information on technical challenges, deployment schedule phasing. The Implementation Plan shall: - Deliver solutions that include a significant portion of the technical infrastructure early in the schedule, without compromising the quality or inherent security of the solution. This should also validate the design and architecture. - Expose technically challenging areas of the project as soon as possible. - Deliver customized functionality to the State in incremental pieces that are in logical business application sequence.	Y		
H11	1	78	H11.1.78	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall describe the interface management approach and methodology used for the solution.	Y		

H11	1	79	H11.1.79	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall incorporate the interface management approach into a comprehensive Interface Management Plan. The Interface Management Plan will be used by the State to document the plan for integrating the solutions with all systems internal and external to the State. The Interface Management Plan shall, at a minimum, document the following areas: - The approach to developing and managing internal and external Solution interfaces. - Technical tools that will be used for data transformation, transport and error recovery. - Tasks, deliverables and resources necessary to complete interface development and implementation. - Description of how the solution development and test systems will work with the external interfaces. - References to applicable sections in the relevant design documents that describe how the solution will be synchronized with the specific internal and external interfaces. - References to applicable sections in the detailed design that describe the mappings between internal and external solution data. - Descriptions of the process for managing changes to the interfaces, both in the production and non-production environments - Interface(s) needed for maintaining data synchronization between an interim production Solution and the final production implementation. - Solution interfaces, data format, frequency of updates and expected data volume. - Process for interfacing and collaborating with interface partners, including roles, responsibilities, deliverables and timelines. - How the State development and test systems shall work with the external non-production interfaces. - Interface tools	Y		
H11	1	80	H11.1.80	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall validate that each interface is working correctly. Project teams (vendor-supplied or otherwise) will repair all interface-related problems caused by Offeror-developed interfaces.	Y		
H11	1	81	H11.1.81	Maintenance and Operations	non-functional	Project teams (vendor-supplied or otherwise) shall assist the State in identifying root causes for all solutions' interface related problems.	Y		
H11	1	82	H11.1.82	Maintenance and Operations	non-functional	Solutions will leverage permitted hosting environments to support their respective technology needs	Y		
H11	1	83	H11.1.83	Maintenance and Operations	non-functional	Solutions will use automated deployment tools and techniques to build, manage and synchronize different environments	Y		
H11	1	84	H11.1.84	Maintenance and Operations	non-functional	Solutions will ensure that environments are synchronized to ensure adequate pre-production testing	Y		
H11	1	85	H11.1.85	Maintenance and Operations	non-functional	Solutions will use an integrated date advancement and rollback feature in training and testing environments	Y		
H11	1	86	H11.1.86	Maintenance and Operations	Contractor	the hosting provider shall provide planned outage notification within the limits defined by the Exchange.	Y		
H11	1	87	H11.1.87	Maintenance and Operations	non-functional	Application and technology components must allow for user analytics to be captured and reported	Y		
H11	1	88	H11.1.88	Maintenance and Operations	non-functional	Application and technology components shall support session replication to support transparent fail over.	Y		
H11	1	89	H11.1.89	Maintenance and Operations	non-functional	Application and technology components should be implemented using the Oracle stack (a.k.a. Oracle Fusion Middleware) and related components	Y		
H11	1	90	H11.1.90	Maintenance and Operations	non-functional	Solutions requiring a JEE server should utilize Oracle WebLogic Server	Y		
H11	1	91	H11.1.91	Maintenance and Operations	non-functional	Application Server shall enable deployment of mission-critical applications or components in a robust, secure, highly available, and scalable environment	Y		
H11	1	92	H11.1.92	Maintenance and Operations	non-functional	Application Server clusters shall provide scalability and reliability for applications by distributing the work load among multiple instances of the Server	Y		
H11	1	93	H11.1.93	Maintenance and Operations	non-functional	Application server shall provide overload protection to allow the Server the ability to detect, avoid, and recover from overload conditions.	Y		
H11	1	94	H11.1.94	Maintenance and Operations	non-functional	Application server shall prioritize work based on pre-defined rules and by monitoring actual run time performance statistics	Y		
H11	1	95	H11.1.95	Maintenance and Operations	non-functional	Application server shall support store-and-forward services to enable the Server to deliver messages reliably between applications that are distributed across many Server instances	Y		
H11	1	96	H11.1.96	Maintenance and Operations	non-functional	Application server shall allow System Administration that include tasks such as creating Application Server domains; deploying applications or components; migrating domains from development environments to production environments; monitoring and configuring the performance of the application Server domain; and diagnosing and troubleshooting problems	Y		
H11	1	97	H11.1.97	Maintenance and Operations	non-functional	The Application Server security architecture shall provide a comprehensive, flexible security infrastructure designed to address the security challenges of making applications or components available on the Web	Y		
H11	1	98	H11.1.98	Maintenance and Operations	non-functional	The application server shall provide for a monitoring and diagnostic service that creates, collects, analyzes, archives, and accesses diagnostic data generated by a running server and its deployed applications	Y		
H11	1	99	H11.1.99	Maintenance and Operations	Solution	The solution shall provide the ability to support commonly used Internet browsers with backwards compatability as defined by the Exchange.	Y		
H11	1	100	H11.1.100	Maintenance and Operations	Solution	The solution shall utilize a service management framework such as ITIL v3 or equivalent framework to manage IT services and infrastructure.	Y		
H11	1	101	H11.1.101	Maintenance and Operations	Solution	The solution must include hosting services for the development, testing/verification, training, certification and production environments that will be used to develop, maintain, and operate the solution.	Y		
H11	1	102	H11.1.102	Maintenance and Operations	Solution	The solution shall provide a standardized mechanism for Conflict Management and data integrity.	Y		
H11	1	103	H11.1.103	Maintenance and Operations	Solution	The contractor shall completely test and apply patches for all third-party software products before release.	Y		

H11	1	104	H11.1.104	Maintenance and Operations	Solution	The Contractor shall notify the Customer prior to the application of any testing or application of modifications to third-party software products	Y		
H11	1	105	H11.1.105	Maintenance and Operations	Solution	The contractor shall ensure that non-critical system management, virtualization, and administrative operational and system administration controls are isolated on the network layer that would contain protected health information (PHI) to prevent unnecessary administrative access to PHI.	Y		
H11	1	106	H11.1.106	Maintenance and Operations	Solution	The system shall utilize industry standard security protocols for transmitting data over networks (e.g. SSL, TLS, etc.)	Y		
H11	1	107	H11.1.107	Maintenance and Operations	Solution	The contractor shall implement network protection capabilities to detect and eliminate malicious software and/or unauthorized external connection attempts on network monitoring devices, servers, peripheral devices, and desktop workstations.	Y		
H11	1	108	H11.1.108	Maintenance and Operations	Contractor	The contractor shall provide all hosting services at data center(s), including back-up and recovery, at sites located within the United States.	Y		
H11	1	109	H11.1.109	Maintenance and Operations	Contractor	The contractor shall ensure that all data center operations and technical staff shall be located within the continental (CONUS) United States.	Y		
H11	1	110	H11.1.110	Maintenance and Operations	Contractor	The contractor is required to host, maintain, and operate the solution in production for the contract term.	Y		
H11	1	111	H11.1.111	Maintenance and Operations	Contractor	The contractor will be responsible for providing, installing, and maintaining all hardware, software, network components, and other infrastructure elements for the solution.	Y		
H11	1	112	H11.1.112	Maintenance and Operations	Contractor	The contractor shall maintain reliable business operations in accordance with the agreed upon SLA.	Y		
H11	1	113	H11.1.113	Maintenance and Operations	Contractor	The Contractor shall provide a system with response times and transaction volume as defined by agreed upon SLA.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Hosting Governance

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H12	1	1	H12.1.1	Hosting Governance	Governance	Hosting Provider will establish Governance Services that are designed to provide a formal management framework and structure that enables Hosting Provider and Customer to manage their relationship, expectations, and dependencies with respect to the Hosting Services.	Y		
H12	1	2	H12.1.2	Hosting Governance	Governance	Governance Services consist of account management, service management, and project management. The success of the governance relationship is dependent upon the effective ongoing engagement of both Hosting Provider and Customer. The Governance framework is supported by a documented set of standards and processes as described in this Schedule.	Y		
H12	1	3	H12.1.3	Hosting Governance	Governance	Hosting Provider will manage the Customer relationship through a series of planning, execution, and review activities. These activities support service level management, availability management, and capacity management under the Hosting Provider Services.	Y		
H12	1	4	H12.1.4	Hosting Governance	Governance	Hosting Provider and Customer will determine the level of Governance Services that is required to support the Environment based on the complexity of Customer's business requirements and/or the types of Hosting Provider Services purchased by Customer.	Y		
H12	1	5	H12.1.5	Hosting Governance	Governance	The services performed by Hosting Provider shall include project planning, development, transition, migration, implementation, configuration services, or any customization or Upgrades of the Hosting Provider Programs. Hosting Provider is responsible for supporting or performing services for any customizations or CEMLIs in the Environment or for managing Service Requests related to functional issues.	Y		
H12	1	6	H12.1.6	Hosting Governance	Governance	Hosting Provider will provide Governance Services that are delivered and managed via the agreed upon delivery methodologies (e.g., remote or onsite) and frequency through Customer agreement.	Y		
H12	1	7	H12.1.7	Hosting Governance	Account Logistics Management	Hosting Provider and Customer will work together to coordinate executive meetings between Hosting Provider and Customer.	Y		
H12	1	8	H12.1.8	Hosting Governance	Account Plan Management	Hosting Provider will produce an Account Management Plan	Y		
H12	1	9	H12.1.9	Hosting Governance	Account Plan Management	Account Management Plan will identify a Hosting Provider and Customer Management Leads who will serve as primary points of contact for Governance Services for the number of days indicated in the Governance Services.	Y		
H12	1	10	H12.1.10	Hosting Governance	Account Plan Management	Hosting provider shall work with Customer's change control board to plan and schedule strategic business and technology events that affect delivery of the service.	Y		
H12	1	11	H12.1.11	Hosting Governance	Account Plan Management	Hosting Provider will aid Customer in creating and chartering a change control board that consists of personnel from its business and IT departments who are authorized to make decisions on behalf of their respective departments. The change control board will make decisions on behalf of Customer as needed with respect to the Hosting Provider Services.	Y		
H12	1	12	H12.1.12	Hosting Governance	Account Plan Management	Ensure that Customer's change control board works and cooperates with Hosting Provider to plan and schedule strategic business and technology events that affect delivery of the Hosting Provider Services.	Y		
H12	1	13	H12.1.13	Hosting Governance	Account Plan Management	Hosting Provider will interact as a member of Customer's change control board meetings.	Y		
H12	1	14	H12.1.14	Hosting Governance	Account Reporting Management	Provide Account Reviews detailing services delivered and identifying potential additional services that may facilitate the Hosting Provider Services.	Y		
H12	1	15	H12.1.15	Hosting Governance	Availability Management	Hosting Provider will coordinate tactical business and technology events with Customer for the purpose of minimizing the impact to the availability of Customer's Production Environment.	Y		
H12	1	16	H12.1.16	Hosting Governance	Availability Management	Hosting Provider will provide an availability plan to Customer detailing Production Environment availability.	Y		
H12	1	17	H12.1.17	Hosting Governance	Availability Management	Hosting Provider will track and monitor Planned Outages and Unplanned Outages in an effort to meet availability targets identified in the availability plan.	Y		
H12	1	18	H12.1.18	Hosting Governance	Availability Management	Hosting Provider will provide the status of Root Cause Analysis for Severity Level 1 Unplanned Outages.	Y		
H12	1	19	H12.1.19	Hosting Governance	Availability Management	Hosting Provider will establish a suitable governance structure to support on-going projects and the operation of Customer's Production Environment.	Y		
H12	1	20	H12.1.20	Hosting Governance	Capacity Management	Hosting Provider will work with Customer to identify additional software and/or infrastructure that may be required based on changes to Customer's business requirements.	Y		
H12	1	21	H12.1.21	Hosting Governance	Capacity Management	Hosting Provider will work with Customer to integrate required changes into the Production Environment.	Y		
H12	1	22	H12.1.22	Hosting Governance	Capacity Management	Hosting Provider will provide capacity information when Customer requests changes to the Production Environment. Examples of the types of requested changes are adding users or storage capacity.	Y		
H12	1	23	H12.1.23	Hosting Governance	Capacity Management	Hosting Provider will provide and maintain the infrastructure requirements, including capacity and usage volumetric information as applicable.	Y		
H12	1	24	H12.1.24	Hosting Governance	Contract Ammendment	Hosting Provider will identify events and/or scenarios that may require that Customer purchase additional Hosting Provider licenses, services and/or infrastructure.	Y		
H12	1	25	H12.1.25	Hosting Governance	Project Management	Hosting Provider will schedule Hosting Provider-initiated changes to infrastructure, such as changes to hardware or network, to minimize impact on key business events identified by Customer.	Y		
H12	1	26	H12.1.26	Hosting Governance	Project Management	Hosting Provider will prepare, manage and report status, as appropriate, on project plans for infrastructure events initiated by Hosting Provider.	Y		
H12	1	27	H12.1.27	Hosting Governance	Project Management	Hosting Provider will perform Hosting Provider-assigned activities and tasks for infrastructure events initiated by Hosting Provider and/or Customer.	Y		
H12	1	28	H12.1.28	Hosting Governance	Service Escalation Management	Hosting Provider will assist Customer with escalating a Hosting Provider Service Request as needed.	Y		
H12	1	29	H12.1.29	Hosting Governance	Service Escalation Management	Hosting Provider will track and monitor any formally escalated Hosting Provider Service Requests and RFCs through to resolution.	Y		
H12	1	30	H12.1.30	Hosting Governance	Service Escalation Management	Hosting Provider will manage escalated Service Requests and RFCs arising from or related to Hosting Provider-initiated infrastructure events.	Y		
H12	1	31	H12.1.31	Hosting Governance	Service Management	Hosting Provider will Produce and articulate a Service Management Plan	Y		
H12	1	32	H12.1.32	Hosting Governance	Service Management	Hosting Provider will work with Customer to plan and schedule tactical business and technology events, such as software patching, maintenance, or Minor Releases.	Y		
H12	1	33	H12.1.33	Hosting Governance	Service Management	Hosting Provider will provide Service Plans to Customer detailing the schedule of tactical events.	Y		
H12	1	34	H12.1.34	Hosting Governance	Service Management	Hosting Provider will communicate process information regarding Change Management, Release Management, and other delivery processes that affect Customer.	Y		

H12	1	35	H12.1.35	Hosting Governance	Service Management	Hosting Provider will track and monitor execution of scheduled events.	Y		
H12	1	36	H12.1.36	Hosting Governance	Service Management	Hosting Provider will track dates for Customer's key planned business and technology events. Hosting Provider will aid Customer in giving appropriate advance notice as required to accommodate lead times in accordance with Hosting Provider Release Management processes.	Y		
H12	1	37	H12.1.37	Hosting Governance	Service Management	Hosting Provider will coordinate Customer's internal Change Management and Release Management processes with Hosting Provider processes.	Y		
H12	1	38	H12.1.38	Hosting Governance	Service Management	Hosting Provider will monitor and measure the operational performance of the Hosting Provider Services.	Y		
H12	1	39	H12.1.39	Hosting Governance	Service Management	Hosting Provider will identify, prepare and facilitate completion of corrective action plans designed to address the operational performance of the Hosting Provider Services.	Y		
H12	1	40	H12.1.40	Hosting Governance	Service Reporting Management	Hosting Provider will provide Customer with service reports, detailing the delivery of the Hosting Provider Services.	Y		
H12	1	41	H12.1.41	Hosting Governance	Service Reporting Management	Hosting Provider will coordinate Service Reviews, per the Governance Services to review the service reports with Customer.	Y		
H12	1	42	H12.1.42	Hosting Governance	Service Request and Request for Change Management	Hosting Provider will provide a process so Customer may request a Change to the Hosting Provider Services via the Change Management process (a "Request for Change" or a "RFC").	Y		
H12	1	43	H12.1.43	Hosting Governance	Service Request and Request for Change Management	Hosting Provider will monitor and assist Customer with progressing Service Requests and RFCs that Hosting Provider and Customer have mutually agreed to monitor,	Y		
H12	1	44	H12.1.44	Hosting Governance	Service Request and Request for Change Management	Hosting Provider will upon Customer's request and subject to the Governance Services, provide Hosting Provider Service Request Reviews, detailing the status and progress of Customer-initiated Service Requests.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Service Level Agreement SLA

Basic	Level	Sub	Req ID Name	Focus	Section	Requirement Description	Requirement Fulfilled?	Notes	Evidence
H13	1	1	H13.1.1	Hosting SLA Definition	Hosting, SLA	Hosting Providers shall create and maintain Service Level Agreements (SLA) that describes the processes and obligations with respect to the availability of, and resolution of incidents for, the programs for which Computer and Administration Services are provided, including specific service levels for performance and availability.	Y		
H13	1	2	H13.1.2		Hosting, SLA,	In the event that multiple Service Levels have been missed and are determined to share the same root cause, Customer is entitled solely to the highest applicable Service Level Credit, rather than accumulated Service Level Credits across all missed Service Levels.	Y		
H13	1	3	H13.1.3	Non-production Availability SLA	Hosting, SLA, Application Availability (Non-Production)	The availability required for non-production applications shall be 99.5%	Y		
H13	1	4	H13.1.4	Production Availability SLA	Hosting, SLA, Application Availability (Production/DR)	The availability required for production applications shall be 99.9%	Y		
H13	1	5	H13.1.5		Hosting, SLA, Application Availability Service Level (Production)	The Application Availability Service Level consists of the measurement of the percentage of time that the Production Environments are available for access and use by Customer to conduct business operations.	Y		
H13	1	6	H13.1.6		Hosting, SLA, Basis for Calculation of Service Level Credits	If Hosting Provider's performance of the Computer and Administration Services in a given month does not meet an applicable Service Level, Customer may be eligible to receive a Service Level Credit. Service Level Credits shall be calculated clearly in the SLA.	Y		
H13	1	7	H13.1.7	Credit Criteria	Hosting, SLA, Credit Criteria	If the monthly performance measured for each Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit	Y		
H13	1	8	H13.1.8		Hosting, SLA, Determining Service Request Severity Level (Adherence to Severity Level Definitions)	Hosting Provider and Customer shall establish a documented a process to assure that the assignment and adjustment of any Severity Level designation is accurate based on the current impact of the reported incident on Customer's use of the Hosting Provider Programs for business operations.	Y		
H13	1	9	H13.1.9	Service Request Severity Level Modification	Hosting, SLA, Determining Service Request Severity Level (Down Grade of Severity Level)	During the Service Request process, the incident no longer warrants the Severity Level currently assigned to it based on its current impact on Customer's ability to use the Hosting Provider Programs for its business operations, then the Severity Level may be downgraded to a lower Severity Level that most accurately reflects the actual current impact.	Y		
H13	1	10	H13.1.10	Initial Service Request Severity Level	Hosting, SLA, Determining Service Request Severity Level (Initial Severity Level)	Hosting Provider and/or Customer shall set the initial Severity Level of a Service Request when submitting the SR via Hosting Provider Support, using defined Severity definitions. If a Service Request is created automatically by monitoring systems or other Tools, or otherwise initiated by Hosting Provider, an Initial Severity Level will be assigned in accordance with SLA. Hosting Provider's Initial focus, upon acceptance of a Service Request, will be to resolve the issues underlying the Service Request. The Severity Level of a Service Request may be upgraded or downgraded.	Y		
H13	1	11	H13.1.11		Hosting, SLA, Determining Service Request Severity Level (Up Grade of Severity Level)	During the Service Request process, the incident warrants the assignment of a higher Severity Level than that currently assigned based on its current impact on Customer's ability to use the Hosting Provider Programs for its business operations, then the Severity Level may be upgraded to a higher Severity Level that most accurately reflects the actual current impact.	Y		
H13	1	12	H13.1.12	Planned Outage	Hosting, SLA, Downtime Exceeds Anticipated Planned Outage Period	If, during a Planned Outage, it is determined that maintenance activities will require an extension of the period of time for such Planned Outage, Hosting Provider will be required to request an extension of such Planned Outage period (including an extension of the Maintenance Window) to accommodate the maintenance activities.	Y		
H13	1	13	H13.1.13	Data Center Location	Hosting, SLA, Hosting Provider Service Level Credit Earn Backs	Hosting Provider Environment(s) shall reside on Infrastructure located at Hosting Provider's continental (CONUS) U.S. Data Center(s). Hosting Provider will provide you with no less than 90 days advance written notice in the event that Hosting Provider relocates the Infrastructure on which your Environment resides to a third party Data Center.	Y		
H13	1	14	H13.1.14		Hosting, SLA, Maintenance	Customer may contact Hosting Provider's Hosting Provider Service Desk to provide Hosting Provider with additional information concerning an outstanding Service Request, in accordance with the following chart. Severity Level Hours of Operation of the Hosting Provider Hosting Provider Service Desk Support Hours ENGLISH(24x7x365) via phone, internet	Y		
H13	1	15	H13.1.15	Maintenance Window Availability	Hosting, SLA, Performance Against Statement of Work Service Level	During agreed to Minor Maintenance Windows, the Production Environments will be available.	Y		
H13	1	16	H13.1.16	Maintenance Window Availability	Hosting, SLA, Performance Against Statement of Work Service Level	During agreed to Major Maintenance Windows (twice annually), the Production Environments may be unavailable.	Y		
H13	1	17	H13.1.17	Emergency Maintenance	Hosting, SLA, Reporting	In the event that emergency maintenance is required, hosting provider(s) will provide advance notification of the maintenance. Unavailability of any Production Environment or Non-Production Environment due to the application of an emergency Change shall be considered a Planned Outage.	Y		
H13	1	18	H13.1.18		Hosting, SLA, Service Level Credit Allocation	Hosting Provider will make available to Customer measurements and reports concerning Hosting Provider's performance against the Application Availability and Service Request Resolution Time Service Levels.	Y		
H13	1	19	H13.1.19	Service Levels and Formulas	Hosting, SLA, Service Request Process	The performance of the Computer and Administration Services shall be measured against the following three Service Levels: Application Availability, Service Request Resolution Time, and Performance Against Statement of Work.	Y		
H13	1	20	H13.1.20	Service Request Process	Hosting, SLA, Service Request Process	Hosting Providers shall establish the Service Request process which provides for diagnosis and resolution of incidents reported in connection with the Hosting Provider Services. Either Hosting Provider or Customer may submit SRs as part of the Service Request process. Hosting Provider monitoring systems may also automatically generate SRs as alerts so that Hosting Provider and Customer may proactively take steps to avoid the potential occurrence of an incident.	Y		
H13	1	21	H13.1.21	Service Request Process	Hosting, SLA, Service Request Resolution Time Service Level	Hosting Provider will follow the a predefined Service Request process, including related tasks and obligations.	Y		
H13	1	22	H13.1.22	Service Request Escalation	Hosting, SLA, Service Request Resolution Time Service Level	Hosting Provider will escalate Service Requests per the a predefined Service Request escalation process	Y		
H13	1	23	H13.1.23	Service Request Resolution Time Monitoring	Hosting, SLA, Service Request Resolution Time Service Level	The Service Request Resolution Time Service Level shall be measured on a monthly basis for each SR Severity Level and calculated in accordance with the following formula:	Y		
H13	1	24	H13.1.24		Hosting, SLA, Service Request Resolution Time Severity Level 1	For purposes of calculating Hosting Provider's performance against the Service Request Resolution Time Service Level or calculating any Service Level Credits, the measurement of Hosting Provider's time-to-resolve shall begin at applicable Service Request creation.	Y		
H13	1	25	H13.1.25	Severity 1 Resolution Time	Hosting, SLA, Severity Level Definitions (Level 1)	The resolution time for severity 1 outages shall be 4 hours (Unplanned Outage caused by Infrastructure and/or application component); <98% of SRs resolved within target	Y		
H13	1	26	H13.1.26	Severity 2 Resolution Time	Hosting, SLA, Severity Level Definitions (Level 1)	The resolution time for severity 2 outages shall be 48 hours; <98% of SRs resolved within target	Y		
H13	1	27	H13.1.27	Severity Level 1	Hosting, SLA, Severity Level Definitions (Level 1)	Severity level 1 shall be defined as an unplanned outage of a production environment where mission-critical business operations cannot reasonably continue and the situation is an emergency. Additional conditions include infrastructure outage, component failure, environment unavailable, data corruption resulting in an operational halt, or an environmental "hang" with no response. All components, software, and interfaces being hosted by a hosting provider.	Y		
H13	1	28	H13.1.28	Severity Level 2	Hosting, SLA, Severity Level Definitions (Level 4)	Severity level 2 shall be defined as an unplanned outage of a non-production environment or a service interruption in a production environment causing critical impact to use of hosted software in one area of the business but not resulting in infrastructure outage.	Y		
H13	1	29	H13.1.29	Severity Level 3	Hosting, SLA, SLA Measurement Exclusions (Only Covers Production/DR)	Severity level 3 shall be defined as an error in expected or documented functionality severely impacting the business operations with no acceptable workaround. Business operations can continue in a restricted fashion	Y		

H13	1	30	H13.1.30	Severity Level 4	Hosting, SLA, SLA Measurement Exclusions (Production Go-Live)	Severity level 4 shall be defined as minor or no loss in expected or documented functionality which may be requests for information, enhancements, or clarification	Y			
H13	1	31	H13.1.31		Hosting, SLA, SLA Measurement Exclusions (Stabalization Period)	Service Levels will be measured and reported during the production phase, and Customer's eligibility to receive Service Level Credits shall be in accordance with the terms of this Schedule.	Y			
H13	1	32	H13.1.32		Hosting, SLA, Stabilization Period	Service Levels will not be measured and do not apply prior to Production Go-Live, and Service Level Credits will not be paid to Customer.	Y			
H13	1	33	H13.1.33		Hosting, SLA, Stabilization Period (length)	Service Levels will be measured and reported during a Stabilization Period, but Service Level Credits will not be paid during such period.	Y			
H13	1	34	H13.1.34		Hosting, SLA, Stabilization Period (not required)	The Hosting Provider has a Stabilization Period that is a ramp period following Changes to a Production Environment.	Y			
H13	1	35	H13.1.35		Hosting, SLA, Stabilization Period (required)	Each Stabilization Period will be ninety (30) calendar days in duration, commencing on the day that the Change is first made to the applicable Production Environment. However, depending on the nature of the Change and the impact on the applicable Production Environment, Hosting Provider and Customer will, as part of the Change Management process, mutually agree on a Stabilization Period of different scope or duration. For purposes of measuring and reporting Hosting Provider's performance against Service Levels and calculating any applicable Service Level Credits for a calendar month in which a Stabilization Period occurs: (1) the Stabilization Period shall be deemed to commence on the first day of such calendar month; and (2) the Stabilization Period shall be deemed to end on the last day of such calendar month.	Y			
H13	1	36	H13.1.36		Hosting, SLA, Stabilization Period (required)	The following Changes may not require a Stabilization Period: The application of Maintenance Code Releases, including the application of tax updates, Mandatory operating system fixes or patches, Mandatory operating system fixes or patches, Changes to equipment or infrastructure managed by Hosting Provider, Database fixes or patches, System maintenance required to maintain levels of functionality or security that is neither requested by, nor caused by Changes made by, Customer.	Y			
H13	1	37	H13.1.37	Stabilization Period	Hosting, SLA, Updates on Resolution Progress	A Stabilization Period will be required for the following types of changes: initial implementation, point releases and major upgrades of software, introduction of CEMLIs, introduction of 3rd party software, and additional modules	Y			
H13	1	38	H13.1.38	Service Request Status Visibility	Hosting, SLA, What Severity Levels Count	The service request and related processes shall support visibility such that submitters and other interested parties may review the progress of the service request	Y			
H13	1	39	H13.1.39	Service Request Monitoring	Hosting, SLA, What Severity Levels Count	Hosting Provider(s) will proactively monitor, and regularly communicate to Customer on, the status of Severity Level 1 Unplanned Outage or Service Interruption Service Requests.	Y			
H13	1	40	H13.1.40			Service Level Credits related to Hosting Provider's performance of the Computer and Administration Services against the Application Availability Service Level shall be calculated in accordance with the service level credit calculation	Y			
H13	1	41	H13.1.41			The Contractor shall be held accountable to issue resolution standards as defined by the agreed upon SLA.	Y			TC-62
H13	1	42	H13.1.42			Solutions shall provide Service Level Agreement (SLA) monitoring and reporting capabilities.	Y			O4.3
H13	1	43	H13.1.43			The contractor shall conduct non-routine maintenance during a mutually agreeable timeframe as defined by the agreed upon SLA.	Y			TC-70
H13	1	44	H13.1.44			The contractor shall provide routine maintenance periods as defined by the agreed upon SLA.	Y			TC-69

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Security Summary

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence	Source
S1	1	1	S1.1.1	SOV		Hosting Provider will follow State of Vermont Secuirty Standards. http://dii.vermont.gov/Policy_Central	Y			
S1	1	2	S1.1.2	General Security		Hosting Provider and Solutions shall comply with General Security standards outlined in S2A Security General and S2B Security General work sheets.	Y			
S1	1	3	S1.1.3			Hosting Provider and Solutions shall comply with Federal Security standards outlined in S3 Federal Security work sheets.	Y			
S1	1	4	S1.1.4	FIPS 199 Standards		Hosting Provider will ensure Security controls of the Federal Security Services align with the functional requirements of a high-impact security category under FIPS 199.	Y			
S1	1	5	S1.1.5	DoD Standards		Solutions shall comply with DoD Directive 8552.01	Y			
S1	1	6	S1.1.6	FISMA Standards		Solutions shall comply with Federal Information Security Management Act (FISMA) of 2002	Y			
S1	1	7	S1.1.7	NIST Standards		Hosting Provider and Solutions shall comply with NIST standards outlined in S4A NIST 800 Series Summary and S4B NIST 800 Series Detail work sheets.	Y			
S1	1	8	S1.1.8	NIST Standards		Hosting Provider will provide certified Infrastructure based on NIST 800-37, utilizing a combined security requirements framework consisting of controls in both NIST Special Publication 800-53 and DoD Directive 8500.2.	Y			
S1	1	9	S1.1.9	NIST DoD Standards		Hosting Provider will align with the portions of NIST 800-37 and DoD Instruction 8510.01. Certification and Accreditation methodology, applicable to hosting providers performance of the services for all Infrastructure and shared services components that reside in the Federal Environment(s).	Y			
S1	1	10	S1.1.10	NIST DoD Standards		Hosting Provider will conduct assessments based on security controls described in NIST 800-53 and DOD 8500.2.	Y			
		11		HIPAA Standards		Hosting Provider and Solutions shall comply with HIPAA standards oulined in S5 HIPAA worksheet.	Y			
S1	1	12	S1.1.12	HIPAA Standards		(a) HIPAA administrative simplification. To the extent that the Exchange performs electronic transactions with a covered entity, the Exchange must use standards, implementation specifications, operating rules, and code sets adopted by the Secretary in 45 CFR parts 160 and 162. (b) HIT enrollment standards and protocols. The Exchange must incorporate interoperable and secure standards and protocols developed by the Secretary in accordance with section 3021 of the PHS Act. Such standards and protocols must be incorporated within Exchange information technology systems.	Y			
S1	1	13	S1.1.13	HITECH Standards		Solutions shall comply with the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009	Y			
S1	1	14	S1.1.14	ACA		Solutions shall comply with the Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations	Y			
S1	1	15	S1.1.15			Hosting Provider and Solutions shall comply with PHI and Privacy standards outlined in S6 PHI and Privacy work sheets.	Y			
S1	1	16	S1.1.16			Hosting Provider and Solutions shall comply with IRS 1075 standards outlined in S7 IRS 1075 and Privacy work sheets.	Y			
S1	1	17	S1.1.17	FTI		Solutions shall comply with the Safeguards for Protecting Federal Tax Returns and Return Information (26 U.S.C. § 6103 and related provisions).	Y			
S1	1	18	S1.1.18	PCI DSS		Hosting Provider and Solutions shall comply with PCI/DSS standards outlined in S8 PCI and Privacy work sheets. Solutions using credit/debit or other electronic funds transfer cards shall be compliant with Payment Card Industry (PCI) security standards	Y			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Security General

Section	Subsection	Sub	Req Number	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Deliverable	Source
S2A	1	1	S2A.1.1	Security General	HIPAA	Hosting provider shall facilitate quarterly meetings shall be conducted between Hosting Provider and Customer to (i) review delivery of the services, (ii) identify any changes in HIPAA regulations, Vermont's business or ePHI Environments that may impact effectiveness or compliance of the service, and (iii) identify any additional services required to address new risks.	Y			
S2A	1	2	S2A.1.2	Security General		Database Audit provides database activity logging, monitoring, and reporting of the production database instances of the Hosting Provider ePHI Environments while protecting audit trails using Hosting Provider's Audit Vault Server and Hosting Provider's Audit Vault Collection Agent program in Vermont's Environment. Included in the service are audit reports and Hosting Provider's recommendations on database events to be collected. Hosting Provider will work with Vermont to include additional unique database logging and auditing requirements in the Database Audit services.	Y			
S2A	1	3	S2A.1.3	Security General		Automated audit mechanisms (e.g., activity logging, monitoring, and reporting) shall be employed on databases. Audit reports shall be included with the hosting provider's recommendations.	Y			
S2A	1	4	S2A.1.4	Security General		Strong Authentication is designed to provide enhanced protection against unauthorized access to Vermont's web application environments using Hosting Provider's adaptive access capabilities. The service shall review of Vermont's business and security requirements to implement appropriate Hosting Provider adaptive access policies and will be implemented in Vermont's selected Non-Production Environment within the identified Enhanced Security Services Environments. Production implementation will take place upon Vermont's successful testing and sign off on the service in a Non-Production Environment.	Y			
S2A	1	5	S2A.1.5	Security General		Data Masking is designed to obscure specific data elements and shall be used in non-production databases in Vermont's Hosting Provider ePHI Environments, by replacing actual, sensitive data identified by Vermont with false, simulated data. The objective of the service is to prevent ePHI contained in specific database fields, from being disclosed to unauthorized parties.	Y			
S2A	1	6	S2A.1.6	Security General		Database data shall be encrypted at the file system layer	Y (at the VM)			
S2A	1	7	S2A.1.7	Security General		Hosting Provider will create and review a security assessment checklist to be included in Vermont's Periodic Maintenance Plan. In addition, Hosting Provider will review the scan results from the QualysGuard scans provided in the Base Services and include recommendations for updates, including any recommendations for remediation to any identified vulnerabilities, in Vermont's Periodic Maintenance Plan.	Y			
S2A	1	8	S2A.1.8	Security General		Hosting Provider will conduct annual reviews of Vermont's Hosting Provider Hosting Provider network router configurations.	Y			
S2A	1	9	S2A.1.9	Security General		Hosting Provider will conduct an annual network and application penetration test for Vermont's Production Hosting Provider ePHI Environment and provide a report on the results of the network and application penetration test to Vermont.	Y			
S2A	1	10	S2A.1.10	Security General		The hosting provider shall monitor, alert, and protect against web application attacks of internet-facing applications. Hosting Provider will install, configure, and manage a web application firewall on Vermont's internet-facing Hosting Provider ePHI Environments.	Y			
S2A	1	11	S2A.1.11	Security General		All data stored on file systems shall be encrypted.	Y (at the VM)			
S2A	1	12	S2A.1.12	Security General		Audits shall be at Vermont's expense. Any request for Hosting Provider to provide assistance with an audit is considered a separate service if such audit assistance requires the use of different or additional resources beyond that which Hosting Provider uses to provide the services in accordance with existing agreements such as audit software or additional employees or subcontractors. Hosting Provider will seek Vermont's written approval and agreement to pay any related fees before performing such audit assistance.	Y			
S2A	1	13	S2A.1.13	Security General		HIPAA Security Services consist of the deployment of certain security controls designed to protect the confidentiality, integrity and availability of Vermont's electronic PHI (ePHI) that may reside in Vermont's Environment within Hosting Provider's Data Center(s). The services are designed to help Vermont meet its legal obligations under the Health Insurance Portability and Accountability Act of 1996 and its regulations ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act"), that may apply to Hosting Provider Hosting Provider's management of Vermont's hosted environments that may contain ePHI. The HIPAA Security Services may be modified from time to time pursuant to the Change Management process in order to reflect changes in industry standards or legal obligations, as determined by Hosting Provider.	Y			
S2A	1	14	S2A.1.14	Security General		Hosting services shall be delivered and managed remotely by Hosting Provider, 24 hours a day, 7 days a week, 365 days a year.	Y			
S2A	1	15	S2A.1.15	Security General		Hosting provider(s) shall conduct an annual risk assessment of ePHI environments against the HIPAA controls to ensure compliance and provide findings to Vermont	Y			
S2A	1	16	S2A.1.16	Security General		Hosting Provider ePHI Environments shall be included in HIPAA Compliance assessment performed by a qualified third party auditor, and provide Vermont with the summary information from the third party assessment report.	Y			
S2A	1	17	S2A.1.17	Security General		Hosting provider shall conduct quarterly QualysGuard scans of Vermont's externally accessible web service on the Production Environment, and provide QualysGuard reports on the scans, including the severity of the vulnerabilities and remediation recommendations.	Y			
S2A	1	18	S2A.1.18	Security General		Hosting provider shall create and provide to Vermont, a network diagram with connections to ePHI, including any wireless networks and connected entities.	Y			
S2A	1	19	S2A.1.19	Security General		Hosting provider shall deploy, monitor and manage third party host-based Data Loss Prevention (HDLP) software on the Windows workstations of Hosting Provider support personnel. The HDLP software is designed to monitor Hosting Provider Hosting Provider DBA and system administration activity and alert for, or block, potential unauthorized access to Vermont's ePHI.	Y			
S2A	1	20	S2A.1.20	Security General		Hosting provider shall provide Operating System management to protect against dictionary and brute force attacks.	Y			
S2A	1	21	S2A.1.21	Security General		Access to ePHI Servers shall be restricted to those employees who have completed HIPAA training.	Y			
S2A	1	22	S2A.1.22	Security General		Hosting Provider will conduct quarterly reviews of the firewall policies and network devices configurations for Vermont's Hosting Provider ePHI Environments.	Y			

S2A	1	23	S2A.1.23	Security General		Network router configurations shall be reviewed annually	Y			
S2A	1	24	S2A.1.24	Security General		Hosting provider shall monitor for, and provide alerts of, unauthorized changes to certain system and application files that would be a sign of a possible Environment compromise. As part of the service, Hosting Provider will perform file integrity monitoring on Vermont's servers within the Hosting Provider ePHI Environments following the file integrity monitoring policies agreed upon by Hosting Provider and Vermont.	Y			
S2A	1	25	S2A.1.25	Security General		An internal and external QualysGuard assessment shall be performed quarterly to understand vulnerabilities in Vermont's Environment and includes quarterly external and internal QualysGuard scans of the servers hosting Vermont's Production Environment and QualysGuard reports on the scans.	Y			
S2A	1	26	S2A.1.26	Security General		Strong authentication shall be employed in all deployment environments	Y			
S2A	1	27	S2A.1.27	Security General		Self-registered users of applications shall have identities verified per NIST SP800-63	Y			
S2A	1	28	S2A.1.28	Security General		HBE-related solutions shall proof identities based on requirements set forth by CMS	Y			
S2A	1	29	S2A.1.29	Security General		Solutions shall have the ability to assign users to multiple OMS (Organization Management System) organizations with different applications and roles	Y			
S2A	1	30	S2A.1.30	Security General		Solutions shall have the ability to manage atomic-to-composite role mappings	Y			
S2A	1	31	S2A.1.31	Security General		Solutions shall have the ability to provide better performance for applications that use fine-grained policies (built security)	Y			
S2A	1	32	S2A.1.32	Security General		Solutions shall support Federal Identity, Credential, and Access Management ("FICAM") Roadmap and Implementation Guidelines	Y			
S2A	1	33	S2A.1.33	Security General		Solutions shall support Protection of PII data	Y			
S2A	1	34	S2A.1.34	Security General		Solutions shall integrate with federal security services for identity proofing and multi-factor authentication	Y			
S2A	1	35	S2A.1.35	Security General		module design and implementation must take into account security standards and controls as documented by NIST	Y			
S2A	1	36	S2A.1.36	Security General		Project participants and other individuals shall not transmit any personally identifiable contract data in non-secure transmissions over the Internet or any wireless communication device, unless: 1) the Contract Data are "de-identified" in accordance with 45 C.F.R § 164.514(b) (2); or 2) encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies and procedures established by the University or the Covered Entity (ies).	Y			
S2A	1	37	S2A.1.37	Security General		All solutions will adhere to applicable standard Privacy and Security Practices.	Y			
S2A	1	38	S2A.1.38	Security General		Solutions will provide a mechanism to securely authorize staff and customers to access the authorized functionality.	Y			
S2A	1	39	S2A.1.39	Security General		Solutions will define the level of access that will be granted to each particular role.	Y			
S2A	1	40	S2A.1.40	Security General		The system will utilize encryption algorithms and implementations, in compliance with National Institute of Standards and Technology.	Y			
S2A	1	41	S2A.1.41	Security General		The system will have a potential fraud detection function.	Y			
S2A	1	42	S2A.1.42	Security General		Solutions will define by department, role, and/or individual employee/user, the access levels and privilege set to create, read, update/change, or delete data. This includes definitions at the customer level.	Y			
S2A	1	43	S2A.1.43	Security General		Solutions will define the data elements displayed to users based on privilege set/ role	Y			
S2A	1	44	S2A.1.44	Security General		User privileges shall be periodically audited	Y			
S2A	1	45	S2A.1.45	Security General		Solutions will identify and define access roles for cross-organizational information systems.	Y			
S2A	1	46	S2A.1.46	Security General		Solutions will ensure the interfaces use the appropriate security protocol per the classification of data being exchanged with external partners	Y			
S2A	1	47	S2A.1.47	Security General		Solutions will log all unsuccessful login attempts.	Y			
S2A	1	48	S2A.1.48	Security General		Application and technology components shall integrate and rely on the centralized IdM infrastructure	Y			
S2A	1	49	S2A.1.49	Security General		The contractor shall ensure that the solution and Service Center complies with all applicable State Information Security Policy (Rev. November 13, 2009).	Y			
S2A	1	50	S2A.1.50	Security General		The system will enforce a single system identify for each unique user involved with the Exchange	Y			
S2A	1	51	S2A.1.51	Security General		The solution will be able to establish family or household linkages between individual accounts.	Y			
S2A	1	52	S2A.1.52	Security General		The solution shall provide intrusion detection and prevention services.	Y			
S2A	1	53	S2A.1.53	Security General		The solution shall provide Certificate Authority for secure server side transactions.	Y			
S2A	1	54	S2A.1.54	Security General		The solution shall provide a complete user provisioning and de-provisioning solution to support achievement of the privacy and security requirements as defined by the Exchange.	Y			
S2A	1	55	S2A.1.55	Security General		The solution shall support user account authenticaion procedures with configurable parameters (time, cipher strength, logon attempts, etc.).	Y			
S2A	1	56	S2A.1.56	Security General		The solution shall support account retirement and deactivation requirements as determined by Exchanbe identity management policies and procedures.	Y			
S2A	1	57	S2A.1.57	Security General		The solution shall support issue and manage public key certificates for secure transactions.	Y			
S2A	1	58	S2A.1.58	Security General		The solution shall support the ability to verify and validate system identity via public key certificates for secure transactions.	Y			

S2A	1	59	S2A.1.59	Security General		The solution shall support the ability to delegate or utilize 3rd party authentication services for specific transactions via an external trust and authentication	Y			
S2A	1	60	S2A.1.60	Security General		The solution shall comply with industry standards and regulations to include, but not limited to the following: Privacy and transaction standards, Federal civil rights laws, Standards adopted by the Secretary under Section 1104 of the Affordable Care Act (ACA), Standards and protocols adopted by the Secretary under Section 1561 of the ACA including NIST SP 800-52, 800-53i, 800-77, or 800-113 or others as specified in the federal Information Processing Standards (FIPS) Publication 140-2, AND IEEE standards and PMI guidelines.	Y			
S2A	1	61	S2A.1.61	Security General		The solution shall support penetration testing from external vendors.	Y			
S2A	1	62	S2A.1.62	Security General		The solution shall maintain strict access controls to safeguard all areas where Exchange data could be accessed.	Y			
S2A	1	63	S2A.1.63	Security General		The sholution shall implement correct plans from internal and external risk assessment and vulnerability testing and/or external (3rd Party) HIPAA audit/review that discusses threats, vulnerabilities and impacts, including network and web application.	Y			
S2A	1	64	S2A.1.64	Security General		The solution shall implement a provisiong, review, and de-provisioning scheme for user identification, authentication and authorization, including activation and de-activation.	Y			
S2A	1	65	S2A.1.65	Security General		The solution shall manage user profiles including defining access to data types and security credentials.	Y			
S2A	1	66	S2A.1.66	Security General		The solution shall allow users to reset passwords and unlock locked accounts from a web portal interface.	Y			
S2A	1	67	S2A.1.67	Security General		The solution shall pass credentials for authentication and authorization from the Exchange solution to authenticate system access to web service transactions.	Y			
S2A	1	68	S2A.1.68	Security General		The solution shall restrict access to user, provider, or organizational data to authorized users.	Y			
S2A	1	69	S2A.1.69	Security General		The solution shall ensure non-repudiation* as part of digital signature verification to prevents data from being altered, deleted or damaged during exchange.	Y			
S2A	1	70	S2A.1.70	Security General		The solution shall have the ability to set automatic alerts to system administrators when a breach pattern or unauthorized use activity is detected.	Y			
S2A	1	71	S2A.1.71	Security General		The solution shall support "user exits" or a "pluggable authentication module" (PAM) to enable user transition between the solution and local systems that are authorized as third party connections to the solution.	Y			
S2A	1	72	S2A.1.72	Security General		The solution shall implement and support two-factor authentication (i.e. two kinds of evidence).	Y			
S2A	1	73	S2A.1.73	Security General		The solution shall provide the ability for web service providers and service consumers to interact via the solution.	Y			
S2A	1	74	S2A.1.74	Security General		The solution shall provide the ability to implement security for transport and messaging via web services.	Y			
S2A	1	75	S2A.1.75	Security General		The solution shall track all access so that an Accounting Of Disclosures report can be provided to the individual if requested.	Y			
S2A	1	76	S2A.1.76	Security General		The solution shall provide the ability disable accounts as defined in the agreed upon SLA.	Y			
S2A	1	77	S2A.1.77	Security General		The solution shall provide security administration functionality to apply user permissions based on roles to accommodate access controls that align with federal (ANSI) standards for Role Based Access Controls.	Y			
S2A	1	78	S2A.1.78	Security General		The solution shall ensure that all health information in transit and at rest is unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified by the Secretary of the Federal Department of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5) , or any update to that guidance.	Y			
S2A	1	79	S2A.1.79	Security General		The solution shall provide the same security provisions for the development, system test, acceptance test and training environment as those used in the production environment.	Y			
S2A	1	80	S2A.1.80	Security General		The contractor shall ensure that the Exchange solution system documentation is protected from unauthorized access.	Y			
S2A	1	81	S2A.1.81	Security General		The Contractor shall define all initial user security roles and access permissions as defined by the State to ensure users are able to access the system at system go-live.	Y			
S2A	1	82	S2A.1.82	Security General	CHIP Compliano	Module design must take into account Medicaid and Child Health Insurance Program privacy protections specified under Code of Federal Regulations (CFR), Title 42, sections 431.300 to .307 and 457.1110.	Y			
S2A	1	83	S2A.1.83	Security General	FIMA Complian	Modules must also comply with the Federal Information Security Management Act of 2002 (FISMA).	Y			
S2A	1	84	S2A.1.84	Security General	HIPAA Complia	Modules must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security and privacy requirements, including standards soon to be promulgated	Y			
S2A	1	85	S2A.1.85	Security General	Existing Identit	Healthcare-related solutions shall utilize or comply with existing data field, validation methods, and policies for identity management.	Y			
S2A	1	86	S2A.1.86	Security General		Solutions shall support identification, authentication, and authorization management.	Y			
S2A	1	87	S2A.1.87	Security General		Public facing solutions shall provide a mechanism for customers to register for an account.	Y			
S2A	1	88	S2A.1.88	Security General		Public facing solutions shall allow customers to manage their user account.	Y			
S2A	1	89	S2A.1.89	Security General		Solutions shall provide a mechanism to control user access.	Y			
S2A	1	90	S2A.1.90	Security General		Solutions shall provide a mechanism to authenticate users.	Y			
S2A	1	91	S2A.1.91	Security General		Solutions and security-related technology components shall provide a mechanism to administer password policies.	Y			
S2A	1	92	S2A.1.92	Security General		Solutions shall support administration password policies.	Y			
S2A	1	93	S2A.1.93	Security General		Solutions will secure data to maintain customer privacy.	Y			
S2A	1	94	S2A.1.94	Security General		The system will gather, store and maintain, as confidential, personal income data to establish eligibility for coverage (i.e., income tax returns, Social Security number).	Y			

S2A	1	95	S2A.1.95	Security General		The system will gather, store, and maintain, as confidential, information necessary to determine individual eligibility for a Qualified Health Plan, regardless of whether the individual qualifies for an Exemption to purchase or enroll.	Y			
S2A	1	96	S2A.1.96	Security General		Solutions will comply with relevant security laws, policies, processes and standards.	Y			
S2A	1	97	S2A.1.97	Security General		Solutions will ensure that data is secured and only accessible to authorized individuals	Y			
S2A	1	98	S2A.1.98	Security General		Solutions will safeguard computer systems, peripherals and assets.	Y			
S2A	1	99	S2A.1.99	Security General		Solutions will protect customer information from unauthorized disclosure.	Y			
S2A	1	100	S2A.1.100	Security General	Directory Attribute Naming	Directory attributes shall conform to VT naming standards and core set of attributes	Y			
S2A	1	101	S2A.1.101	Security General	Virtual Directory Services	IdM solutions shall be implemented with a virtual directory to improve maintainability	Y			
S2A	1	102	S2A.1.102	Security General	Directory Separation	Separate directories shall be used for employees and external users. Additional directory segmentation TBD	Y			
S2A	1	103	S2A.1.103	Security General	Directory LDAP Accessibility	Directories shall be accessible via the LDAP protocol	Y			
S2A	1	104	S2A.1.104	Security General	SSO	Solutions shall utilize SSO components for authentication and authorization	Y			
S2A	1	105	S2A.1.105	Security General		The Solution shall have role based access control at the data field level	Y			
S2A	1	106	S2A.1.106	Security General		The Solution shall have the capability to automatically deactivate staff/employee account if there has been no log-in for a specified time (e.g. 90 days)	Y			
S2A	1	107	S2A.1.107	Security General	CMS	The vendor will complete and supply to the Customer all CMS Security required documentation to include but not limited to System Security Plan (SSP), Risk Assessment (RA), Contingency Plan (CP).	Y			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Security General B

Base	Level	Sub	Req ID	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence	Source
S2B	1	1	S2B.1.1	Hosting, General Security Services		Security assessments shall be performed prior to releasing solutions into production	Y			
S2B	1	2	S2B.1.2	Hosting, General Security Services,		Hosting Provider will determine the appropriate classification for Vermont data.	Y			
S2B	1	3	S2B.1.3	Hosting, General Security Services,		Hosting Provider will determine the appropriate levels of control for Vermont data.	Y			
S2B	1	4	S2B.1.4	Hosting, General Security Services,		Failure of an employee to adhere to the Hosting Provider Data Privacy Policy and Information Security Policy may result in disciplinary action in accordance with Hosting Provider policies.	Y			
S2B	1	5	S2B.1.5	Hosting, General Security Services,		If Vermont's regulatory obligations require it to perform an audit of computer systems storing Vermont's data, Vermont's Management Lead must provide a written request to the hosting provider with information detailing the requested scope of the audit and the regulatory obligation necessitating the audit. If a Third Party Vendor is to conduct the audit, the Third Party Vendor must be mutually agreed to by Vermont and Hosting Provider. The third party auditor is required to execute a written confidentiality agreement acceptable to Hosting Provider before conducting the audit.	Y			
S2B	1	6	S2B.1.6	Hosting, General Security Services,		[illegible] and Statement of Work and for the sole purpose of assisting Vermont with its need to comply with its regulatory requirements. At least six weeks in advance of the proposed audit date, Vermont must submit to hosting provider a detailed audit plan describing the proposed scope (subject to the terms above), duration, and start date of the audit. Hosting Provider will review the audit plan and provide Vermont with any concerns or questions about the plan (for example, any request for information that could compromise Hosting Provider security, privacy, or employment policies). Hosting Provider will work cooperatively with the Vermont to agree on a final audit plan.	Y			
S2B	1	7	S2B.1.7	Hosting, General Security Services,		Audits shall be conducted during regular business hours, subject to Hosting Provider policies and regulations, and may not unreasonably interfere with Hosting Provider business activities.	Y			
S2B	1	8	S2B.1.8	Hosting, General Security Services,		Hosting Provider shall acknowledge that Vermont may be subject to audits by entities other than regulators. If the information required for such an audit is not contained in a SSAE 16 or ISAE 3402 report, Hosting Provider will make reasonable efforts to provide the required information to the auditor, provided that the auditor signs a confidentiality agreement acceptable to Hosting Provider and such requests for information occur no more frequently than once each year.	Y			
S2B	1	9	S2B.1.9	Hosting, General Security Services,		Vermont will provide hosting provider with any audit reports generated in connection with any audit of the Hosting Provider Services, unless prohibited by law. Vermont may use the audit reports only for the purposes of meeting its regulatory audit requirements. The audit reports are confidential information of the parties under the terms of the Agreement.	Y			
S2B	1	10	S2B.1.10	Hosting, General Security Services, Access Control		Access to logs shall be provided on a need to know and Least Privilege basis. Log files should be protected by SHA1 cryptographic hash sum and are monitored. Logs on intranet-accessible systems are relocated daily to systems that are not intranet- accessible.	Y			
S2B	1	11	S2B.1.11	Hosting, General Security Services, Access Control		Access control shall refer to the policies, procedures, and Tools that govern the access to and use of resources within Vermont's Environment. Examples of resources include, but are not limited to, a physical Server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol.	Y			
S2B	1	12	S2B.1.12	Hosting, General Security Services, Access Control		Least Privilege shall be employed for all solutions. It is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.	Y			
S2B	1	13	S2B.1.13	Hosting, General Security Services, Access Control Policy		Default-deny is a network-oriented approach that implicitly denies the transmission of all network traffic, and then specifically allows only required network traffic based on protocol, port, source, and destination.	Y			
S2B	1	14	S2B.1.14	Hosting, General Security Services, Access Control to Program Source Code		Prior to deployment, all new deployments of technology or software in the Hosting Provider Data Centers shall undergo a security technical review by a cross-organization team including a dedicated security team. Technology or tools that do not meet Hosting Provider's security policies or standards shall not deployed.	Y			
S2B	1	15	S2B.1.15	Hosting, General Security Services, Annual Testing		The incident commander is responsible for making sure appropriate reports are generated after each security incident. Two commonly used reports are a Root Cause Analysis and Investigation report.	Y			
S2B	1	16	S2B.1.16	Hosting, General Security Services, Annual Testing		The ISIRP is tested at least once, but not more than twice, every twelve months. Information Security Incident Response management appoints an ISIRC to conduct the testing. Chief-Level (e.g. a CEO, a CIO or a CTO) executive approval is required for unscheduled testing.	Y			
S2B	1	17	S2B.1.17	Hosting, General Security Services, Annual Testing		The hosting provider shall periodically test its incident response procedures under the direction of an incident commander. At the conclusion of each test, the commander must submit a gap analysis report to incident response management along with recommendations for corrective actions.	Y	Need to discuss frequency of this as it could affect costs for personnel		
S2B	1	18	S2B.1.18	Hosting, General Security Services, Asset Classification and Control		Hosting Provider will maintain a Hosting Provider Information Security Policy which describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Hosting Provider. Includes governing principles such as 'need to know', Least Privilege, and segregation of duties. All employees, contractors and temporary employees are subject to the Hosting Providers Information Security Policy.	Y			
S2B	1	19	S2B.1.19	Hosting, General Security Services, Asset Control Responsibilities		Upon termination of services, hosting provider shall return information held in paper form to Vermont or destroyed in accordance with the Hosting Provider Information Protection Policy.	Y			
S2B	1	20	S2B.1.20	Hosting, General Security Services, Audits		Vermont remains solely responsible for its regulatory compliance in its use of Hosting Provider Services. Vermont should make Hosting Provider aware of any technical requirements that result from its regulatory obligations prior to contract signature. Hosting Provider will work with Vermont to determine whether Hosting Provider Hosting Provider Services are consistent with those requirements. Additional fees may apply.	Y			
S2B	1	21	S2B.1.21	Hosting, General Security Services, Backup and Recovery Procedure		HIPAA Security Services are required to have the following controls in place on the desktops and laptops used to connect to ePHI environments: Anti Virus, Full disk encryption, removeable media encryption and host data loss prevention	Y			
S2B	1	22	S2B.1.22	Hosting, General Security Services, Backup and Recovery Procedure		[illegible] combination of disk and tape backups to protect Vermont data. Procedures are in place for regular backup protection with a defined timeline and scheduling. Backups of Vermont data take place using dedicated backup servers and tape libraries. Unless otherwise required by law, backup tapes are labeled and shipped to a secure, fire-safe off-site storage vault facility managed by a Payment Card Industry (PCI) Data Security Standard certified Third Party Vendor where they are retained in accordance with requirements. The backup tapes are transported to the off-site facility on a daily basis by the third party storage vendor. Processes for archiving and retrieving material from the off-site storage vendor are documented.	Y			
S2B	1	23	S2B.1.23	Hosting, General Security Services, Backup and Recovery Procedure		Hosting provider shall employ the use of dedicated backup servers	Y			
S2B	1	24	S2B.1.24	Hosting, General Security Services, Backup and Recovery Procedure		Hosting provider shall label and ship backup media to a secure, fire-safe, off-site vault location managed by a Payment Card Industry Security standard.	Y			
S2B	1	25	S2B.1.25	Hosting, General Security Services, Backup and Recovery Procedure		Backup media shall be shipped to the off-site facility on a daily basis	Y			
S2B	1	26	S2B.1.26	Hosting, General Security Services, Backup and Recovery Procedure		Processes for archiving and retrieve backup media from off-site storage shall be documented and followed	Y			
S2B	1	27	S2B.1.27	Hosting, General Security Services, Backup and Recovery Procedure		The data stored in the backup tapes is encrypted using strong cryptography (AES-256 bit) and a True Random Number Generator (TRNG) for the generation of strong keys for each tape where the keys are unique to Vermont. Vermont will be provided a process to decrypt encrypted tapes. Administrative access to the key management system is role-based. Administrators of multiple systems are required to make material changes to the key management system. Keys are maintained in more than one U.S. Data Center.	Y			
S2B	1	28	S2B.1.28	Hosting, General Security Services, Backup and Recovery Procedure		All backup media shall be encrypted using strong cryptography (AES-256) and a True Random Number Generator (TRNG).	Y			
S2B	1	29	S2B.1.29	Hosting, General Security Services, Backup and Recovery Procedure		Administrative access to key management system is role-based.	Y			
S2B	1	30	S2B.1.30	Hosting, General Security Services, Backup and Recovery Procedure		Encryption keys are maintained in more than one Data Center located in the contiguous United States ("lower 48", CONUS).	Y			

S2B	1	31	S2B.1.31	Hosting, General Security Services, Breach Policy		Vermont is provided with Servers and storage that are physically and logically isolated from the Servers and storage of other Hosting Provider customers Access controls are multi-tiered, consisting of the network, system, database and application layers. All access is authorized on a Default-deny basis.	Y			
S2B	1	32	S2B.1.32	Hosting, General Security Services, Breach Policy		Third-party hosting services (i.e, servers, storage) shall be physically separated and logically isolated from other customers' components.	Y			
S2B	1	33	S2B.1.33	Hosting, General Security Services, Breach Policy		Access controls to network, system, database, and application layers shall be multi-tiered and accessible on a default-deny basis	Y			
S2B	1	34	S2B.1.34	Hosting, General Security Services, Breach Policy		Hosting providers shall share relevant Breach, Security, or Enforcement policies	Y			
S2B	1	35	S2B.1.35	Hosting, General Security Services, Chain of Custody		and control of incident response efforts. A core team evaluates, contains, eradicates, and recovers from security incidents and a communications team identifies, coordinates, and develops pertinent communications for internal parties. An extended team consists of senior management in corporate communications (PR), legal, Human Resources, privacy, and security and identifies, coordinates and develops pertinent communications for external parties, including any legally required reporting. An advanced incident support team completes security assessments and digital forensics analysis in an effort to ensure that chain of custody is maintained. The ISIRC is required to submit a lessons-learned report to Information Security Incident Response management at the conclusion of security incident response efforts. ISIRT members involved in the security incident response are encouraged to provide feedback on the lessons learned from each incident.	Y			
S2B	1	36	S2B.1.36	Hosting, General Security Services, Clear Desk and Clear Screen		All desktop and laptop computers purchased by Hosting Provider are pre-loaded with a standard corporate desktop software image called the Hosting Provider Base Image (OBI). The OBI is GIS- approved with screen saver settings configured to lock access to the computer after 10 minutes of inactivity. Only the Hosting Provider user or an administrator can unlock the computer with a valid password required on resume. When desktop and laptop computers are off of Hosting Provider premises and left unattended, they are required to be physically secured.	NO	Not in Scope		
S2B	1	37	S2B.1.37	Hosting, General Security Services, Clear Desk and Clear Screen	Screen Lock	All desktop computers at Vermont, subsidiaries, vendors, or contractors shall have screens lock after 10 minutes of inactivity and require either the user or administrator password to unlock it.	Y			
S2B	1	38	S2B.1.38	Hosting, General Security Services, Cloud Services Risk Management		Hosting Provider shall maintain a Security Organization Policy describing and clarifing the roles and responsibilities of various teams and individuals involved in information security at Hosting Provider, including the executive-level Oversight Committee, Corporate Information, Product, and Physical Security organizations, IT and IT Security organizations, all lines of business (LoBs) and individual Information Security Managers (ISMs) who are assigned by each LoB to represent the security leadership of each organization.	Y			
S2B	1	39	S2B.1.39	Hosting, General Security Services, Communications and Operations Management		Environmental conditions shall be maintained to meet manufacturer recommended specifications for operating temperature, relative humidity and power consumption.	Y			
S2B	1	40	S2B.1.40	Hosting, General Security Services, Compliance with Laws and the European Union Data Privacy Directive		Vermont staff and third-parties shall comply with all applicable data protection laws to the extent that such laws by their terms impose obligations directly on Vermont and third-parties	Y			
S2B	1	41	S2B.1.41	Hosting, General Security Services, Compliance with Laws and the European Union Data Privacy Directive		Vermont shall be responsible to not provide third-parties (i.e., hosting providers) access to health, payment card, or other sensitive personal information requiring specific regulatory, legal, or industry data security obligations	Y			
S2B	1	42	S2B.1.42	Hosting, General Security Services, Compliance with Laws and the European Union Data Privacy Directive		In the event of a lapse of Hosting Provider Safe Harbor status, Hosting Provider will make reasonable efforts to promptly remedy such a lapse.	Y			
S2B	1	43	S2B.1.43	Hosting, General Security Services, Compliance with Laws and the European Union Data Privacy Directive		Hosting Provider and its subsidiaries have subscribed to an agreement under which an Hosting Provider subsidiary handling Vermont data adopts safeguards consistent with those of the Hosting Provider subsidiary contracting with a Vermont for Hosting Provider Services. The Hosting Provider subsidiary contracting with the Vermont is responsible for Hosting Provider compliance and its subsidiaries' compliance with this requirement.	Y			
S2B	1	44	S2B.1.44	Hosting, General Security Services, Confidentiality		Hosting Provider shall use an external screening agency to perform pre-employment background investigations for newly hired U.S. personnel. Contracted physical security personnel are required to pass a criminal and Department of Motor Vehicle background check as well as a drug screen prior to employment.	Y			
S2B	1	45	S2B.1.45	Hosting, General Security Services, Confidentiality Agreements		Hosting Provider shall provide Risk Management Services and is responsible for IT Security strategy, architectural design of security solutions, engineering, risk management, security infrastructure operations and support, standards and compliance, threat intelligence and remediation, and security technical assessment for new infrastructure. Cloud Services Risk Management also facilitates audits, including Vermont and third party compliance reviews.	Y			
S2B	1	46	S2B.1.46	Hosting, General Security Services, Cryptographic Controls	Hosting provider connection methodologies	Hosting Provider shall support a variety of external connection methodologies to provide wide area network (WAN) connectivity between Vermont's Environment and Vermont's networks.	Y			
S2B	1	47	S2B.1.47	Hosting, General Security Services, Data Center Physical Controls		Hosting provider shall have a formal process for employment terminations to ensure sufficient protection of information. After a termination is processed, automated notifications are issued for terminations (regardless of type) based on the effective date of the termination. The recipient list for the notifications includes all necessary parties. Access to systems is terminated immediately and if necessary, escorted off premise.	Y			
S2B	1	48	S2B.1.48	Hosting, General Security Services, Data Center Physical Controls		Hosting provider shall employ an integrated security management system with electronic photo ID badges, cardholder access control, recorded digital video surveillance, and alarm monitoring. Data Centers shall have a single entrance that is manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management. Building perimeters shall use alarm systems and a 24x7 security protection unit.	Y			
S2B	1	49	S2B.1.49	Hosting, General Security Services, Data Center Physical Controls		The hosting provider's integration security management system shall use CCTV system internally and externally with digital video recording.	Y			
S2B	1	50	S2B.1.50	Hosting, General Security Services, Data Center Physical Controls		Information processing, storage, and distribution facilities housed at Hosting Provider's Data Centers are protected by a defined security perimeter with appropriate security barriers and entry controls.	Y			
S2B	1	51	S2B.1.51	Hosting, General Security Services, Data Center Physical Controls		Only employees, Third Party Vendors, and contractors on an approved sponsor list, or visitors with prior approval, are allowed to enter Hosting Provider's Data Centers.	Y			
S2B	1	52	S2B.1.52	Hosting, General Security Services, Data Center Physical Controls		Access to Hosting Provider's Data Centers by visitors must be approved by Data Center senior management in advance of the visit; requests for such visits must include the anticipated duration of the visit.	Y			
S2B	1	53	S2B.1.53	Hosting, General Security Services, Data Center Physical Controls		Hosting Provider data center visitors must provide proof of their identity. Such proof must consist of a photo ID issued by Hosting Provider or a government. The visitor is then documented on a sign-in sheet and issued a temporary badge.	Y			
S2B	1	54	S2B.1.54	Hosting, General Security Services, Data Center Physical Controls		Hosting provider Visitors are banned from possessing weapons, recording devices and alcohol while on Data Center premises.	Y			
S2B	1	55	S2B.1.55	Hosting, General Security Services, Data Center Physical Controls		Hosting provider Visitor badges are inventoried on a nightly basis. Any badge identified as missing will be immediately deactivated.	Y			
S2B	1	56	S2B.1.56	Hosting, General Security Services, Data Center Physical Controls		Hosting Provider Data Center doors shall be linked to a security application running on a secure host. The application is used to zone the building and grant access to areas on an as needed basis. Access lists for each Data Center are reviewed monthly. Upon an employee's termination or transfer from a Data Center, the employee's access privileges are revoked.	Y			
S2B	1	57	S2B.1.57	Hosting, General Security Services, Data Center Physical Controls		Hosting Provider maintains the following physical security standards to prohibit unauthorized physical access at all company facilities from which Vermont's data may be handled ("Service Locations").	Y			
S2B	1	58	S2B.1.58	Hosting, General Security Services, Data Center Physical Controls		Physical access to Hosting provider Service Locations shall be limited to Hosting Providers employees, subcontractors, and authorized visitors.	Y			

S2B	1	59	S2B.1.59	Hosting, General Security Services, Data Center Physical Controls		Hosting Provider employees, subcontractors, and authorized visitors shall be issued identification cards that must be worn while on the premises.	Y			
S2B	1	60	S2B.1.60	Hosting, General Security Services, Data Center Physical Controls		Visitors to Service Locations are required to sign a visitor's register, be escorted and/or observed when they are on the premises, and/or be bound by the terms of a confidentiality agreement.	Y			
S2B	1	61	S2B.1.61	Hosting, General Security Services, Data Center Physical Controls		Hosting Providere Security monitors the possession of keys/access cards and the ability to access the Service Locations. Employees leaving employment must return keys/cards immediately.	Y			
S2B	1	62	S2B.1.62	Hosting, General Security Services, Data Center Physical Controls		After-hours access to Service Locations shall be monitored and controlled by Hosting Provider Security.	Y			
S2B	1	63	S2B.1.63	Hosting, General Security Services, Data Privacy and Security Compliance		The Hosting Provider Chief Privacy Officer and Hosting Provider Legal department, working in conjunction with Hosting Provider security organizations, develop and manage the implementation of and compliance with the Hosting Provider Data Privacy Policies.	Y			
S2B	1	64	S2B.1.64	Hosting, General Security Services, Database Security		All deployment environments shall be configured with the same security and compliance standards whether production or non-production.	Y			
S2B	1	65	S2B.1.65	Hosting, General Security Services, Database Security		Write access to the product databases is restricted to database administrators with the exception that Vermont has the ability to grant an End User access to update interface tables and CEMLI schema objects.	Y			
S2B	1	66	S2B.1.66	Hosting, General Security Services, Database Security		Vermont and its implementer may be granted management rights and write access to Non-Production Environments and, based on role, to the custom database schemas in all environments if compliance and security controls can be maintained.	Y			
S2B	1	67	S2B.1.67	Hosting, General Security Services, Enforcement, Security		Each permanent or contract employee who handles data is required to complete a data privacy awareness training course. The course instructs employees on the definitions of data privacy and personal data, recognizing risks relating to personal data, understanding their responsibilities for data, and reporting any suspected privacy violations. Employees handling data are also required to complete training in corporate ethics. Additionally, employees involved in development of custom code are required to attend secure coding training.	Y			
S2B	1	68	S2B.1.68	Hosting, General Security Services, Environment/Application Security		Vermont shall be responsible for all End User administration within applications.	Y			
S2B	1	69	S2B.1.69	Hosting, General Security Services, Environmental Controls		Hosting Provider Security shall authorize all repairs and modifications to the security barriers or entry controls at Service Locations.	Y			
S2B	1	70	S2B.1.70	Hosting, General Security Services, Exchange of Information		Encrypted tapes and disk drives in servers and mass storage devices are required to be sanitized and destroyed at the end of life. (The sanitization process for encrypted tapes requires deletion of the encryption key in order to make the data stored in the tape unrecoverable. Server disk drives are sanitized by degaussing them. Hosting Provider Data Centers maintain a designated area to store defective or expired media until such media is sanitized and transferred to authorized Third Party Vendors for secure destruction, unless such media is degaussed immediately.)	Y			
S2B	1	71	S2B.1.71	Hosting, General Security Services, Exchange of Information		Encrypted tapes and disk drives in servers and mass storage devices are required to be sanitized and destroyed at end of life.	Y			
S2B	1	72	S2B.1.72	Hosting, General Security Services, Exchange of Information		Encryption keys used for tapes shall be destroyed when tapes are sanitized.	Y			
S2B	1	73	S2B.1.73	Hosting, General Security Services, Exchange of Information		Server disk drives shall be sanitized by degaussing.	Y			
S2B	1	74	S2B.1.74	Hosting, General Security Services, Exchange of Information		Hosting provider data centers shall maintain designated areas to store defective or expired media until sanitized and/or transported to third party for secure destruction	Y			
S2B	1	75	S2B.1.75	Hosting, General Security Services, File Transfer		Designated Hosting Provider personnel handle removable digital media and prepare it for transportation according to defined procedures. Digital media is logged, securely transported, and vaulted by an off-site Third Party Vendor. The vendor is contractually obligated to comply with Hosting Provider-defined terms for media protection. Digital media and printed media are handled in accordance with the Hosting Provider Information Protection Policy.	Y			
S2B	1	76	S2B.1.76	Hosting, General Security Services, Firewalls		Routers shall provide the connection point between Hosting Provider infrastructure and the Internet Service Provider(s) (ISP) facilitating site-to-site VPN connections between Vermont's and Hosting Provider's networks. Border routers are deployed in a fully redundant, fault tolerant configuration connecting to different ISPs. Border Gateway Protocol (BGP) is configured to provide route convergence in the event of an ISP link failure. Routers are deployed with access lists configured to enforce traffic policies at the perimeter adding an additional level of security.	Y			
S2B	1	77	S2B.1.77	Hosting, General Security Services, Harden Network Devices	SSL Load balancing	Server load balancers (SLBs) with built-in SSL accelerators shall be deployed in redundant pairs to offload processor-intensive SSL transactions from Servers and shall be configured as a secure reverse proxy to prevent direct unmonitored access to application Servers on the public middle tier.	Y			
S2B	1	78	S2B.1.78	Hosting, General Security Services, Hardening		A security assessment to identify known operating system vulnerabilities shall be performed against Certified Configurations prior to their release.	Y			
S2B	1	79	S2B.1.79	Hosting, General Security Services, Hardening		Operating system hardening shall be performed in a controlled environment as part of detailed build procedures for Certified Configurations and includes:	Y			
S2B	1	80	S2B.1.80	Hosting, General Security Services, Hardening		All servers shall have operating systems hardened by eliminating any unnecessary system services, accounts, network services, limited user access rights throughout the environments.	Y			
S2B	1	81	S2B.1.81	Hosting, General Security Services, Health Insurance Portability and Accountability Act (HIPAA) Compliance		Vermont may request a copy of the SSAE 16 and ISAE 3402 reports, as applicable, by contacting the hosting provider providing the following information: company name, contact name, title, recipient email address, request justification (purpose)	Y			
S2B	1	82	S2B.1.82	Hosting, General Security Services, Health Insurance Portability and Accountability Act (HIPAA) Compliance		Beginning in February 2010, the Health Insurance Portability and Accountability Act of 1996 and its regulations (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, requires covered entities to ensure that their service providers accessing their electronic PHI (ePHI) take specific security measures to safeguard the data.	Y			
S2B	1	83	S2B.1.83	Hosting, General Security Services, Hosting Provider's Business Continuity Management Program		The hosting provider shall be responsible for collecting and retaining evidence.	Y			
S2B	1	84	S2B.1.84	Hosting, General Security Services, Hosting Provider's Business Continuity Management Program		Hosting Provider shall have a global business continuity management program covering Hosting Provider's staff, information assets, and critical business processes in the event of a natural or man-made crisis or disaster. The program relates specifically to Hosting Provider's internal business continuity, and is implemented through company-wide training, integrated implementation, ongoing testing of emergency response, crisis management, and disaster recovery practices. The program is executed through local, regional, event-specific, and travel-focused crisis management teams.	Y			
S2B	1	85	S2B.1.85	Hosting, General Security Services, Incident Response Plan Growth and Development		Hosting provider shall use a multi-stage process when responding to an incident such as Preparation, Identification, Containment, Eradication, Recovery, and Followup.	Y			
S2B	1	86	S2B.1.86	Hosting, General Security Services, Independent Review of Information Security		All Hosting Provider employees and contractors that may have access to Vermont data shall be subject to a written confidentiality agreement. Prior to performing services for Hosting Provider and prior to accessing any Hosting Provider system or resource, service providers are required to sign a Services Provider Agreement, a Network Access Agreement, and a work order defining the services to be provided.	Y			
S2B	1	87	S2B.1.87	Hosting, General Security Services, Information Access Restriction		Hosting Provider does not restrict the period during which connections to information resources are allowed.	Y			
S2B	1	88	S2B.1.88	Hosting, General Security Services, Information Classification Guidelines		All information assets shall have an owner who is responsible for the protection and inventory of assets based on the sensitivity and value of information. If ownership has not been assigned, it will default to the administrators of the application or system. This includes maintenance of operations guides and other documentation describing the environments.	Y			
S2B	1	89	S2B.1.89	Hosting, General Security Services, Information Disposal		Hosting provider will not disclose Vermont data except in accordance with the Statement of Work, subsequent written instructions by Vermont, or as required by law	Y			

S2B	1	90	S2B.1.90	Hosting, General Security Services, Information Disposal		Upon termination of the services, or at Vermont's request, and following return of a copy of Vermont data, Hosting Provider shall erase Vermont data on any type of information storage systems located at a Hosting Provider facility from which the services are provided in accordance with the Hosting Provider Media Sanitization and Disposal Policy (unless there is a legal obligation imposed on Hosting Provider preventing the deletion of all or part of the data). Vermont's data is erased in a manner designed to destroy boot partitions, file pointers, and user data that resides on the media to prevent the data from being reconstructed and read through ordinary means.	Y				
S2B	1	91	S2B.1.91	Hosting, General Security Services, Information Labeling and Handling		Information assets shall be classified in accordance with the Hosting Providers' Information Protection Policy. The Hosting Provider policy identifies Vermont data as among Hosting Provider's top two categories of confidential information, which have associated limits on access, distribution, and handling. Hosting Provider will keep the information confidential in accordance with security/compliance requirements.	Y				
S2B	1	92	S2B.1.92	Hosting, General Security Services, Information Security Incident Response – Reporting Breaches		Hosting Providers shall subscribe to vulnerability notification systems to stay apprised of security incidents, advisories, and other related information. Hosting Provider shall take actions on the notification of a threat or risk once it has the opportunity to confirm that both a valid risk exists and that the recommended changes are applicable to Hosting Provider environments.	Y				
S2B	1	93	S2B.1.93	Hosting, General Security Services, Information Security Incident Response – Reporting Breaches		whether the data is held on Hosting Provider-, Vermont-, or Third Party Vendor-owned hardware, or on the personal hardware assets of Hosting Provider employees and contingent workers. The hosting provider shall be informed of such Incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those Incidents. The hosting provider will work with Vermont, internal LoBs, the appropriate technical teams, and where necessary, outside law enforcement to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of Vermont's Environment, and to establish root causes and remediation steps.	Y				
S2B	1	94	S2B.1.94	Hosting, General Security Services, Information Security Incident Response – Reporting Breaches		Hosting Provider IT operations staff are instructed in addressing Incidents where handling of data may have been unauthorized, including prompt and reasonable reporting, escalation procedures, and chain of custody practices, to secure relevant evidence.	Y				
S2B	1	95	S2B.1.95	Hosting, General Security Services, Information Security Incident Response – Reporting Breaches		Data breaches shall be reported to Vermont within three business days unless otherwise required by law	Y				
S2B	1	96	S2B.1.96	Hosting, General Security Services, Information Security Incident Response Plan		In the event of a security incident, an incident report will be completed and reviewed with Vermont	Y				
S2B	1	97	S2B.1.97	Hosting, General Security Services, Information Security Incident Response Plan		The hosting provider shall update and maintain an incident response plan periodically for accuracy and effective information security incident response planning. This document is made available to a Information Security Incident Response Team (SIRT) members, systems and network administrators, information security managers, data privacy personnel and business professionals who are responsible for preparing and responding to, information security incidents.	Y				
S2B	1	98	S2B.1.98	Hosting, General Security Services, Information Security Incident Response Plan		With regard to security incidents, information sharing shall be allowed on a need to know basis only.	Y				
S2B	1	99	S2B.1.99	Hosting, General Security Services, Information Security Incident Response Plan		Risk team members shall make detailed records from the onset of data misappropriation Incidents based on pre-defined templates.	Y				
S2B	1	100	S2B.1.100	Hosting, General Security Services, Information Systems Acquisition, Development, and Maintenance		Hosting Provider's policies for use of portable/mobile devices are detailed in the Hosting Provider Acceptable Use Policy for Company Resources and the Wireless Network Policy and apply to all Hosting Provider employees.	Y				
S2B	1	101	S2B.1.101	Hosting, General Security Services, Intrusion Detection		Integrity of the data-in-transit shall be protected through the use of strong encryption (TLS/SSL or IPSec) protocols. Hosting Provider shall configure an nHashed Message Authentication Code - Secure Hash Algorithm (HMAC-SHA-1) on all IPSec VPN networks to verify that the contents of the transmission have not been altered in transit.	Y				
S2B	1	102	S2B.1.102	Hosting, General Security Services, IPSec Virtual Private Network (VPN)	Cryptographic controls IPSec and SSL	Cryptographic controls shall be implemented using IPSec and SSL protocols to provide end users, whether they are Vermont's End Users or Hosting Provider support engineers, with secure access to the target applications.	Y				
S2B	1	103	S2B.1.103	Hosting, General Security Services, IPSec Virtual Private Network (VPN)	VPN	Hosting Provider shall require the implementation of IPSec as part of an overall VPN strategy for securing Vermont data between endpoints on external network connections. IPSec security associations (SAs) are configured using the IP Encapsulating Security Payload (ESP) protocol in tunneling security mode. Key exchange is accomplished through Internet Security Association Key Management Protocol (ISAKMP) using Diffie-Hellman public key techniques with the following IPSec parameters:	Y				
S2B	1	104	S2B.1.104	Hosting, General Security Services, IPSec Virtual Private Network (VPN)	VPN Tunnel	VPN tunnel endpoints shall be encrypted with (minimally) 168-bit Triple DES	Y				
S2B	1	105	S2B.1.105	Hosting, General Security Services, ISO 27001 Certification for the Information Security System		Hosting Provider Hosting Provider has received the ISO 27002 Certificate of Conformance. ISO/IEC 27002 is an internationally recognized standard that assists organizations with selecting and applying controls to information security, predominantly to Information Technology (IT), and provides a framework that takes into account legal, regulatory and contractual requirements.	Y				
S2B	1	106	S2B.1.106	Hosting, General Security Services, ISO 27002 Certificate of Conformance		To help Vermont's meet their security obligations under HITECH, Hosting Provider offers its Hosting Provider HIPAA Security Service. The HIPAA Security Service includes additional security controls that supplement the Practices described herein and are aligned with the standards established by HITECH. Fees for the HIPAA Security Service are separate from, and in addition to, fees for the Computer and Administration Services.	Y				
S2B	1	107	S2B.1.107	Hosting, General Security Services, ISO 27002 Certificate of Conformance		Hosting provider(s) shall comply with HIPAA and HITECH security controls for relevant health care-based components.	Y				
S2B	1	108	S2B.1.108	Hosting, General Security Services, ISO 27002 Certificate of Conformance		Hosting provider shall posess an ISO 27002 Certificate of Conformance.	NO	Not in Scope, not applicable to US Federal SBE needs			
S2B	1	109	S2B.1.109	Hosting, General Security Services, Legal Compliance		The hosting provider's business continuity management program shall address the following in the event of a disaster: Facilitate expedient cross-LoB, internal and external, global communications, Ensure continuity of key functions in a work around manner until normalcy is restored (the new state of normalcy may be unknown and business decisions may need to be made about the service after the crisis is managed), Ensure recovery of computing/technology infrastructure and services.	Y				
S2B	1	110	S2B.1.110	Hosting, General Security Services, Legally Required Disclosures		card data, known as the Payment Card Industry Data Security Standards (PCI DSS). Hosting Provider offers its Hosting Provider Payment Card Industry Compliance Service as an add-on feature to some of its core hosting offerings. The Payment Card Industry Compliance Service can be used to manage a portion of the PCI DSS controls, and provides Vermont access to Hosting Provider partners who may provide additional products and services to assist with Vermont's PCI DSS compliance needs. The Payment Card Industry Compliance Service is assessed annually by a Qualified Security Assessor, and Visa and MasterCard have listed Hosting Provider Hosting Provider as a PCI DSS-compliant Managed Merchant Hosting Service Provider.	Y				
S2B	1	111	S2B.1.111	Hosting, General Security Services, Limitation of Connection Time		Duration of active sessions shall be limited on all VPN, operating system, administrative application, and network device accounts.	Y				
S2B	1	112	S2B.1.112	Hosting, General Security Services, Log Review		Logs with security-relevant information shall be retained for up to three months, and may be kept online or offline. Hosting Provider(s) may choose to expand retention periods, particularly if an anomalous system event or series of events occur that could constitute an information security incident.	Y				
S2B	1	113	S2B.1.113	Hosting, General Security Services, Log Review		Hosting Provider utilizes a Security Information and Event Management (SIEM) system to correlate and alert on Intrusion Detection System security events, firewall log events, and network flow events. The SIEM system is monitored 24 hours per day, seven days per week, 365 days per year.	Y				
S2B	1	114	S2B.1.114	Hosting, General Security Services, Log Security		Hosting Provider shall review logs for forensic purposes and incidents, and any anomalous activities are incorporated into the incident management process.	Y				
S2B	1	115	S2B.1.115	Hosting, General Security Services, Logging		Hosting provider(s) shall dedicate SFTP Servers with dedicated network storage volume for use by Vermont.	Y				

S2B	1	116	S2B.1.116	Hosting, General Security Services, Logging		Hosting Provider(s) shall log security related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to the Environment or Hosting Provider Programs, as well as system alerts, console messages, and system errors. Hosting Provider implements controls to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Security-related log entries shall capture the following information: date, time, time zone, user account name and/or IP address, original value, location of change (hostname, filename, tablename), new value (other than password).	Y			
S2B	1	117	S2B.1.117	Hosting, General Security Services, Media Handling and Disposal		Hosting Provider shall employ intrusion detection systems to provide continuous surveillance for intercepting and responding to security events as they are identified.	Y			
S2B	1	118	S2B.1.118	Hosting, General Security Services, Media Handling and Disposal		Vermont data is not permitted to be stored on any type of removable drive or medium unless the information is encrypted.	Y			
S2B	1	119	S2B.1.119	Hosting, General Security Services, Media Handling and Disposal		Sensitive information in hard copy paper form is required to be disposed of in a shredder or secure disposal container. Electronic data is erased or disposed of in accordance with Hosting Provider's and/or Vermont's Media Sanitization and Disposal Policy.	Y			
S2B	1	120	S2B.1.120	Hosting, General Security Services, Media Handling and Disposal		Vermont, its hosting provider(s), or other partners shall maintain strict restrictions over the internal and external distribution of any kind of media that contains Vermont health information, in accordance with any and all Information Protection Policies, Media Sanitization and Disposal Policies, Hosting Provider Services Privacy Policies, and Hosting Provider Records Retention Policies.	Y			
S2B	1	121	S2B.1.121	Hosting, General Security Services, Media Handling and Disposal		Hosting provider shall use a unique series of tape barcode or other machine readable identification label on all tapes used for backup or other purposes	Y			
S2B	1	122	S2B.1.122	Hosting, General Security Services, Media Handling and Disposal		Hosting provider shall label all tapes used for data or backup purposes as confidential.	Y			
S2B	1	123	S2B.1.123	Hosting, General Security Services, Mobile Computing and Teleworking		All servers instances within an deployment environment are isolated via Firewall based on application role.	Y			
S2B	1	124	S2B.1.124	Hosting, General Security Services, Mobile Computing and Teleworking		Remote access for Hosting Provider employees and subcontractors requires all connections to the Hosting Provider network from a non-Hosting Provider location to use either an IPSec or SSL-encrypted VPN.	Y			
S2B	1	125	S2B.1.125	Hosting, General Security Services, Mobile Computing and Teleworking		Hosting Provider support engineers are required to use 2-factor authentication to authenticate over a VPN through the HPISN to access Vermont's Environment.	Y			
S2B	1	126	S2B.1.126	Hosting, General Security Services, Monitoring		Hosting Provider shall access Vermont's data only for the purpose of providing the services or as required by law, in accordance with the scope of services. Hosting Provider does not and will not: Change Vermont data, other than with Vermont's approval and as required for the performance of the services, have any role in determining or maintaining the accuracy of Vermont data, control Vermont's access to its data, except to the extent that access is restricted via physical and logical access controls as part of the services	Y			
S2B	1	127	S2B.1.127	Hosting, General Security Services, Monitoring		Hosting provider will not monitor Vermont's use of or access to Vermont data except as necessary to provide the services	Y			
S2B	1	128	S2B.1.128	Hosting, General Security Services, Network Access Controls	Screen Positioning	Employees, vendors, and subcontractors are required to position screens to prevent inadvertent visual disclosure and to not leave confidential information unattended or unsecured when not in use.	Y			
S2B	1	129	S2B.1.129	Hosting, General Security Services, Network Connection Control		The Hosting Provider Continuous Connection Network (OCCN) is a multi-tiered DMZ environment, inside a dedicated extranet that is isolated from Hosting Provider's internal corporate network. It functions as a secure access gateway between support systems and targets Vermont applications and database Servers. Three regional gateways, one in the U.S., one in EMEA, and one in APAC, are synchronized in order to provide continuity of support operations in the event one of the gateways fails.	Y			
S2B	1	130	S2B.1.130	Hosting, General Security Services, Network Routing Control		Hosting Provider shall implement authentication, authorization, and accounting through security mechanisms designed to ensure that only approved support engineers with a valid OCCN account can access the Environment using 2-factor authentication through OCCN VPN. Named accounts shall be mapped to individual users and bound to static IP addresses over a VPN. Syslogs shall be used to log and audit all access to the Environment.	Y			
S2B	1	131	S2B.1.131	Hosting, General Security Services, Network Security Management		Restoration of data is tested annually.	Y			
S2B	1	132	S2B.1.132	Hosting, General Security Services, Organizational Security		Hosting Provider security policies shall cover the management of security for both internal operations as well as the services provided to Vermont. The policies apply to all Hosting Provider employees. Specific standards and policies may exceed requirements mandated by general security policies, thus enforcing further controls within Hosting Providers operations and systems. These policies, aligned with the ISO/IEC 27002:2005 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2005 standards, govern all areas of security applicable to hosting services. Security policies relevant to the provision of Hosting Services are available for review.	Y			
S2B	1	133	S2B.1.133	Hosting, General Security Services, Organizational Security Infrastructure		External audits against Hosting Provider Hosting Provider controls will be supplied to Vermont.	Y			
S2B	1	134	S2B.1.134	Hosting, General Security Services, Outbound Internet Access	Network device hardening	Network device configurations shall be hardened by performing the following: Disabling Telnet access, Controlling Simple Network Management Protocol (SNMP) access to devices, Controlling access to devices through the use of Terminal Access Controller Access Control System Plus (TACACS+), turn off unneeded services, perform appropriate level of logging.	Y			
S2B	1	135	S2B.1.135	Hosting, General Security Services, Password Use	Data Usage	All Vermont employees, subsidiaries, vendors (e.g., Hosting Provider(s)) and subcontractors shall observe Hosting Provider policies concerning the treatment of information, including access, use, disclosure, storage, processing, recording, handling, and disposal of Vermont data residing on an Hosting Provider hosted Server.	Y			
S2B	1	136	S2B.1.136	Hosting, General Security Services, Payment Card Industry Data Security Standard		Hosting provider's teams shall have been granted an ISO 27001 Certification for its staff, technology and processes.	NO	Not in Scope, not applicable to US Federal SBE needs		
S2B	1	137	S2B.1.137	Hosting, General Security Services, Physical Media in Transit		Hosting Provider maintains master service agreements with various Third Party Vendors for services and products. Specific controls are defined and agreed upon to secure Vermont data in transit and storage. Hosting Provider maintains a contract with a Third Party Vendor for the transportation and storage of Vermont backup tapes.	Y			
S2B	1	138	S2B.1.138	Hosting, General Security Services, Privilege Management	Privilege Management	Hosting Provider shall provision access through a centralized account provisioning system that is integrated with its human resources database. Access privileges are granted based on job role and require management approval.	Y			
S2B	1	139	S2B.1.139	Hosting, General Security Services, Protection Against Malicious Code		A Production Assessment status report is prepared and provided to Vermont to identify whether Vermont's Environment has been properly prepared.	Y			
S2B	1	140	S2B.1.140	Hosting, General Security Services, Protection Against Malicious Code		Hosting Provider's Desktop and Laptop Security Policy requires that all computers connected to internal network have anti-virus software installed and strongly recommends that employees have a local firewall and desktop asset management software installed. Anti-virus software must be scheduled to perform daily definition updates and virus scans. Additionally, all employees with computers running the Windows operating system are recommended to have the Windows Software Update Service (WSUS) service installed with automatic updates activated.	Y			
S2B	1	141	S2B.1.141	Hosting, General Security Services, Protection Against Malicious Code		All personal computing devices connected to the hosting provider's internal network shall have anti-virus software installed and operational with daily updates to virus definitions and scans. Windows-based computing devices shall have Windows Software Update Services and SMS installed with automated updating.	Y			
S2B	1	142	S2B.1.142	Hosting, General Security Services, Protection Against Malicious Code		Hosting Provider shall keep anti-virus products and WSUS servers up-to-date with virus definitions and security updates. Is responsible for notifying internal system users of any credible virus threats and when WSUS security updates are available.	Y			
S2B	1	143	S2B.1.143	Hosting, General Security Services, Protection Against Malicious Code		Hosting Provider employees shall comply with instructions received through e-mail, and are responsible for promptly reporting to the employee helpdesk any virus, or suspected virus infection that cannot be resolved by anti-virus software.	Y			
S2B	1	144	S2B.1.144	Hosting, General Security Services, Protection Against Malicious Code		Hosting Provider employees shall be prohibited from altering, disabling, or removing anti-virus software and the WSUS service from any computer. Any employee who is discovered violating this standard may be subject to disciplinary action, up to and including termination.	Y			
S2B	1	145	S2B.1.145	Hosting, General Security Services, Protection Against Malicious Code		Hosting provider personnel shall be required to install the approved full disk encryption software on their laptops, which uses a strong encryption algorithm (AES-256). Data on the disk can only be accessed through the use of a private key stored as a password protected file on the disk. A pre-boot login manager allows authorized users to login to unlock the key, boot the operating system, and access the data.	Y			

S2B	1	146	S2B.1.146	Hosting, General Security Services, Protection Against Malicious Code		Hosting Provider Server Security Policy requires all Windows servers to run up-to-date anti-virus software and to have SMS patch management.	Y			
S2B	1	147	S2B.1.147	Hosting, General Security Services, Protection Against Malicious Code		Hosting Provider shall license and install Third Party Vendor anti-virus and anti-spam products to scan all employee and Vermont email and inbound attachments that traverse either Vermont's dedicated servers located at Hosting Provider's Data Centers.	Y			
S2B	1	148	S2B.1.148	Hosting, General Security Services, Protection Against Malicious Code (HIPAA)		Hosting Provider Email infrastructure servers, by default, have "opportunistic encryption" using TLS, which allows encryption on both inbound and outbound emails depending on the capabilities of Vermont's email systems. Vermonts may request to enforce encryption using TLS for its emails traversing the Hosting Providers email infrastructure.	Y			
S2B	1	149	S2B.1.149	Hosting, General Security Services, Responsibility		A chain of custody process shall be used for security incidents to maintain and document the chronological history of evidence. Each person collecting, processing, and handling evidence must record the date and time they received the evidence, and any action taken on the evidence.	Y			
S2B	1	150	S2B.1.150	Hosting, General Security Services, Responsibility, Inventory, and Ownership of Assets		The Hosting Providers Information Protection Policy shall provide guidelines for all Hosting Providers personnel regarding information classification schemes and minimum handling requirements associated with those classifications in an effort to ensure protection of Hosting Proviser and Vermont information assets.	Y			
S2B	1	151	S2B.1.151	Hosting, General Security Services, Review of Access Rights	Database Password Expiry	Database passwords shall be maintained by Hosting Provider operations and changed a minimum of every 180 days.	Y			
S2B	1	152	S2B.1.152	Hosting, General Security Services, Secure Code Training		Hosting Provider will provide any appropriate notices and/or obtain any required consents relating to its collection and use of Vermont data, including any such consents necessary for Hosting Provider to provide the Hosting Provider Services.	Y			
S2B	1	153	S2B.1.153	Hosting, General Security Services, Secure Login Procedures		Firewalls are utilized to control access between the Hosting Provider network and Vermont's network by allowing only authorized traffic using Default-deny. Firewalls are deployed in a layered approach to perform thorough packet inspection with security policies configured to intelligently filter packets based on protocol, port, source, and destination IP address.	Y			
S2B	1	154	S2B.1.154	Hosting, General Security Services, Secure Login Procedures		Access to operating systems shall be controlled by a secure login procedure that requires a unique user ID and a strong password.	Y			
S2B	1	155	S2B.1.155	Hosting, General Security Services, Secure Login Procedures		Root passwords of hosts and facilities must be scheduled to change every 30 days. This applies to any and all servers for Vermont hosted in Vermont or at a third-party hosting provider	Y			
S2B	1	156	S2B.1.156	Hosting, General Security Services, Secure Sockets Layer (SSL)	VPN SSL	Hashed Message Authentication Code - Secure Hash Algorithm (HMAC-SHA-1) shall be used to prevent message corruption with VPN tunnels	Y			
S2B	1	157	S2B.1.157	Hosting, General Security Services, Security Awareness Education and Training		Hosting Provider employees shall be required to maintain the confidentiality of Vermont data. Employees are required to sign a confidentiality agreement and comply with company policies concerning protection of confidential information (Code of Ethics and Business Conduct, Hosting Provider Acceptable Use Policy for Company Resources, and the Information Protection Policy) as part of their initial terms of employment. Hosting Provider obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.	Y			
S2B	1	158	S2B.1.158	Hosting, General Security Services, Security Awareness Education and Training		Hosting Provider shall promote security awareness and educates employees through quarterly newsletters, ad hoc security awareness campaigns, and security-related corporate send mails.	Y			
S2B	1	159	S2B.1.159	Hosting, General Security Services, Security of System Files		The Environments shall undergo a security assessment process that includes review of the Hosting Provider Programs, hardware and operating system components. Finally, any new Releases are installed in a shared staging environment for final validation prior to Production Go-Live.	Y			
S2B	1	160	S2B.1.160	Hosting, General Security Services, Security Requirements Analysis and Specification		Hosting Providers who also develop/integration software/solutions shall have those business units separate from the hosting business unit	Y			
S2B	1	161	S2B.1.161	Hosting, General Security Services, Security Requirements Analysis and Specification		Hosting Provider will deploy Hosting Provider programs through a Certified Configuration which are assessed for exposure to a variety of both common and complex attack types and vulnerabilities.	Y			
S2B	1	162	S2B.1.162	Hosting, General Security Services, Security Requirements Analysis and Specification		The Hosting Provider Programs are deployed on a Server(s) in accordance with the Certified Configuration and/or detailed build procedures. A standard "KickStart" Image is used to install the operating system and a package manager is then used to automatically install the utility programs required for the type of Server being configured. Finally, the file system is built and the Hosting Provider Programs are installed from standard images. Hardening procedures are embedded within a Certified Configuration.	Y			
S2B	1	163	S2B.1.163	Hosting, General Security Services, Security Services		Hosting Provider will limit direct administrative access to Vermont's SBU data residing in the Federal Environment at Hosting Providers Data Center(s) to only those employees who are U.S. citizens. Individuals born in the United States and/or granted citizenship status by Immigration and Naturalization Services (INS) are considered U.S. citizens.	Y			
S2B	1	164	S2B.1.164	Hosting, General Security Services, Segregation in Networks	Outbound network access	Outbound Internet access shall be enabled by default for all hosted Servers within Hosting Provider networks through secure web proxies and restricted portsinbound or direct Internet access from the hosted Servers bypassing web proxies shall not permitted.	Y			
S2B	1	165	S2B.1.165	Hosting, General Security Services, Segregation in Networks	Segregation in Networks	Hosting Provider's Data Centers shall contain (at least) two isolated network environments used to deliver Hosting Services.	Y			
S2B	1	166	S2B.1.166	Hosting, General Security Services, Segregation of Duties		The SOPs describe the detailed activities and tasks undertaken by Hosting Provider employees when delivering services and provide direction for those activities. These SOPs are managed centrally and are available to authorized employees.	Y			
S2B	1	167	S2B.1.167	Hosting, General Security Services, Sensitive System Isolation		Database auditing will be enabled.	Y			
S2B	1	168	S2B.1.168	Hosting, General Security Services, Sensitive System Isolation		Production Environments shall be isolated from Non-Production Environments.	Y			
S2B	1	169	S2B.1.169	Hosting, General Security Services, Sensitive System Isolation		All deployment environments shall be isolated from one another.	Y			
S2B	1	170	S2B.1.170	Hosting, General Security Services, Server load balancers (SLBs)	SSL Certificate Procurement	SSL shall be used for all web-based SSL certified applications. Hosting providers shall procure SSL certificates on Vermont's behalf using VeriSign Corporation as the Certification Authority (CA).	Y			
S2B	1	171	S2B.1.171	Hosting, General Security Services, Session Time Out		Servers shall enable default log file settings for auditing critical events	Y			
S2B	1	172	S2B.1.172	Hosting, General Security Services, SSAE and ISAE Reports and Other Audits		Hosting Provider may store Vermont's contact information, such as names, phone numbers, and e-mail addresses in any country where Hosting Provider does business and may use such information internally and to communicate with Vermont.	Y			
S2B	1	173	S2B.1.173	Hosting, General Security Services, SSAE and ISAE Reports and Other Audits		International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, which was issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB), which is part of the International Federation of Accountants (IFAC); and (b) the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, which was issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in April 2010. ISAE 3402 and SSAE 16 require the completion of detailed testing of controls over a minimum of six months by an independent auditing body.	Y			
S2B	1	174	S2B.1.174	Hosting, General Security Services, SSAE and ISAE Reports and Other Audits		Hosting provider(s) shall regularly undergo third party auditor reviews of production deployments using the standards in the SSAE 16 and ISAE 3402.	Y			
S2B	1	175	S2B.1.175	Hosting, General Security Services, Standard Operating Procedures		Hosting Provider shall align with the IT service management process areas as outlined in the Information Technology Infrastructure Library (ITIL) and uses this framework as a guide for operational delivery. Hosting Provider's internal documentation specifies current operational processes and procedures for employees' performance of technical functions related to all services and environments.	Y			
S2B	1	176	S2B.1.176	Hosting, General Security Services, System Acceptance		Capacity planning and management shall occur throughout the hosting life cycle.	Y			
S2B	1	177	S2B.1.177	Hosting, General Security Services, System Acceptance		Requires the completion of a Production Assessment on Vermont's Environment prior to Production Go-Live. The Production Assessment consists of a series of functional, configuration, supportability, security, and performance tests and is designed to proactively identify and address key issues that may impact system performance following Production Go-Live.	Y			

S2B	1	178	S2B.1.178	Hosting, General Security Services, System Acceptance		The hosting provider shall perform and publish an assessment prior to production go-live to ensure functionality, configuration, supportability, security, and performance are within specification.	Y				
S2B	1	179	S2B.1.179	Hosting, General Security Services, System Acceptance		The Production Assessment team performs system checks and collects documentation in the following areas: Configuration and supportability, Functional system architecture, Security compliance.	Y				
S2B	1	180	S2B.1.180	Hosting, General Security Services, System Passwords	Password Confidentiality	Passwords shall be treated as confidential information.	Y				
S2B	1	181	S2B.1.181	Hosting, General Security Services, System Planning		Hosting Provider shall have security and privacy requirements in its service provider contracts, which address issues such as physical and logical security requirements, privacy protection, breach reporting, and auditing. In addition, as security requirements or services change, subcontractor contracts are changed accordingly upon renewal.	Y				
S2B	1	182	S2B.1.182	Hosting, General Security Services, System Planning		Hosting Provider Certified Configuration systems shall hardened and undergo security assessments. Vermont environments will be deployed with Certified Configurations.	Y				
S2B	1	183	S2B.1.183	Hosting, General Security Services, Terminations		Hosting provider shall conduct Security reviews, assessments, and audits periodically to confirm compliance with the Hosting Providers Information Security Policy, procedures, and practices. Employees who fail to comply with the Information Security Policy, procedures and guidelines may be subject to disciplinary action, up to and including termination.	Y				
S2B	1	184	S2B.1.184	Hosting, General Security Services, Third Party Service Delivery		The hosting provider shall employ separate roles to ensure proper separation of duties	Y				
S2B	1	185	S2B.1.185	Hosting, General Security Services, Unattended Hosting Provider Employee Equipment	Password Confidentiality and Strength	The use of passwords is addressed in the Hosting Provider Password Policy. Hosting Provider employees shall follow rules for password length and complexity and keep their passwords confidential and secure at all times. Passwords shall not be disclosed to any unauthorized person, but under certain circumstances, passwords may be communicated between authorized Hosting Provider employees for the purpose of providing support services.	Y				
S2B	1	186	S2B.1.186	Hosting, General Security Services, Use of System Utilities		Access to the operating system is restricted to named user accounts mapped to individual users with a valid role-based access requirement approved by the user's management through Vermont or a hosting provider's access provisioning process.	Y				
S2B	1	187	S2B.1.187	Hosting, General Security Services, User Authentication for External Connections	User Authentication for External Connections	Hosting Provider shall employ network controls to address the protection and control of Vermont data during its transmission from one end system to another. All computers, Servers, and other data devices connected to the Hosting Provider network must comply with hosting provider standards for security, configuration, and access method, in accordance with the Hosting Provider policies.	Y				
S2B	1	188	S2B.1.188	Hosting, General Security Services, User Identification and Authentication		Operating system access is preceded by identity validation through a login process requiring a unique id and strong password	Y				
S2B	1	189	S2B.1.189	Hosting, General Security Services, User Password Management	User Password Management Dependencies	Authorization shall be dependent on authentication since controlling access to specific resources depends upon establishing an entity or individual's identity. All Hosting Provider authorization decisions for granting, approval, and review of access are based on the following principles: Need to know: does the user require this access for their job function? Segregation of duties: will the access result in a conflict of interest?	Y				
S2B	1	190	S2B.1.190	Hosting, General Security Services, User Password Management	User Password Strong Password Policy	Hosting Provider shall enforce strong password policies for Hosting Provider network, operating system, and database accounts in an effort to reduce the chances of intruders gaining access to the Environment through exploitation of user accounts and their associated passwords.	Y				
S2B	1	191	S2B.1.191	Hosting, General Security Services, User Password Management	Password Strength	Passwords must meet the following characteristics for any software application: Minimum of eight characters long, Contain at least one upper case character and at least one number or special character, Expire every ninety days, Cannot be a common word or name, cannot contain any part of a username.	Y				
S2B	1	192	S2B.1.192	Hosting, General Security Services, User Password Management	Password Strength Audit	Passwords shall be periodically audited to ensure they comply with the Password Strength requirements	Y				
S2B	1	193	S2B.1.193	Hosting, General Security Services, User Registration	User Registration	The Hosting Provider Logical Access Controls Policy is applicable to access control decisions for all Hosting Provider employees and any information processing facility for which Hosting Provider has administrative authority. The policy does not apply to publicly accessible Internet-Facing Hosting Provider systems or Vermont's End Users.	Y				
S2B	1	194	S2B.1.194	Hosting, General Security Services, User Responsibilities	Network OS Account Review	Network and operating system accounts shall be reviewed regularly in an effort to ensure the appropriate employee access levels.	Y				
S2B	1	195	S2B.1.195	Hosting, General Security Services, Vermont Regulatory Compliance		Vermont data located on Hosting Provider systems, including text and images, may be disclosed as required by law without prior consent of Vermont. Hosting Provider will use diligent efforts to inform Vermont, to the extent permitted by law, of any request for such disclosure before disclosure is made.	Y				

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Security General

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence	Source
S3	1	1	S3.1.1	Federal Security	Hosting, Code of Ethics and Business Conduct	The Hosting Provider has a Code of Ethics and Business Conduct document that sets forth Hosting Provider's high standards for moral ethics and business conduct at every level of the organization, and at every location where Hosting Provider does business. The standard applies to Hosting Provider employees, independent contractors, and temporary employees; it covers the areas of legal and regulatory compliance and business conduct and relationships. Compliance-tracked training in ethics and business conduct and sensitive information handling is required once every two years.	YES			
S3	1	2	S3.1.2	Federal Security	General	Hosting Provider will provide dedicated physical and virtual infrastructure to Vermont	YES			
S3	1	3	S3.1.3	Federal Security	General	Hosting Provider will locate Vermont's Environment(s) within a dedicated, caged federal compliant environment ("Federal Environment"), activities related to the operating environment of Programs in the Federal Environment, and the support and Infrastructure for the Federal Environment.	YES			
S3	1	4	S3.1.4	Federal Security	Data Sensitivity Classification	Hosting Provider will provide storage to and provide access to Sensitive But Unclassified Vermont data.	YES			
S3	1	5	S3.1.5	Federal Security	U.S. Citizen Support	Hosting Provider will provide a United States citizen-only support model for access to Vermont data in the Federal Environment.	YES			
S3	1	6	S3.1.6	Federal Security	General	Hosting Provider will provide certified infrastructure based on NIST 800-37, utilizing a combined security requirements framework consisting of controls in both NIST Special Publication 800-53 and DoD Directive 8500.2.	YES			
S3	1	7	S3.1.7	Federal Security	General	Hosting Provider will set up of Vermont's Production Environment, Production Support Environment(s), and Non-Production Environments within the Federal Environment.	YES			
S3	1	8	S3.1.8	Federal Security	General	Hosting Provider will provide Maintenance of the Vermont Federal Environment Infrastructure.	YES			
S3	1	9	S3.1.9	Federal Security	Certification and Accreditation	Hosting Provider will limit data in the Federal Environment to Unclassified data.	YES			
S3	1	10	S3.1.10	Federal Security	Certification and Accreditation	Hosting Provider will align with the portions of NIST 800-37 and DoD Instruction 8510.01. Certification and Accreditation methodology, applicable to hosting providers performance of the services for all Infrastructure and shared services components that reside in the Federal Environment(s).	YES			
S3	1	11	S3.1.11	Federal Security	Certification and Accreditation	Hosting Provider will conduct assessments based on security controls described in NIST 800-53 and DOD 8500.2.	YES			
S3	1	12	S3.1.12	Federal Security	Connectivity to Restricted Networks	Hosting Provider will provide Vermont information and access reasonably needed by Vermont to complete its Vermont Certification and Accreditation.	YES			
S3	1	13	S3.1.13	Federal Security	Connectivity to Restricted Networks	Hosting Provider will provide appropriate connection approval process if additional connectivity to resitricted networks is required.	YES			
S3	1	14	S3.1.14	Federal Security	Data Sensitivity Classification	Hosting Provider will ensure Federal Security Services are designed to align with Mission Assurance Category (MAC) Level I security policies.	YES			
S3	1	15	S3.1.15	Federal Security	Data Sensitivity Classification	Hosting Provider will set security policies for data that is Sensitive But Unclassified (SBU). Federal Environment is not required to store or process Classified data.	YES.			
S3	1	16	S3.1.16	Federal Security	DoD Mission Assurance Category	Hosting Provider will provide a description of the functional properties of the controls used on the Federal Environment. The description of the functional properties of the controls is intended to provide sufficient detail to permit analysis and testing of the controls.	YES			
S3	1	17	S3.1.17	Federal Security	General	Hosting Provider will ensure Federal Security Services are available for all Disaster Recovery Services and Environments.	YES			
S3	1	18	S3.1.18	Federal Security	General	Hosting Provider will ensure Security controls of the Federal Security Services align with the functional requirements of a high-impact security category under FIPS 199.	YES			
S3	1	19	S3.1.19	Federal Security	Certification and Accreditation	Hosting Provider will be responsible for the cost and execution of additional security certification documentation and testing if such activities are required for government approval of connection to restricted networks.	YES			

Base	Level	Sub	Req ID New	Focus	Specifics
	00		AC-00	Access Control	Access Control Group
	01		AC-01	Access Control	AC-01
	02		AC-02	Access Control	AC-02
	03		AC-03	Access Control	AC-03
	04		AC-04	Access Control	AC-04
	05		AC-05	Access Control	AC-05
	06		AC-06	Access Control	AC-06
	07		AC-07	Access Control	AC-07
	08		AC-08	Access Control	AC-08
	09		AC-09	Access Control	AC-09
	10		AC-10	Access Control	AC-10
	11		AC-11	Access Control	AC-11
	12		AC-12	Access Control	AC-12
	13		AC-13	Access Control	AC-13
	14		AC-14	Access Control	AC-14
	15		AC-15	Access Control	AC-15
	16		AC-16	Access Control	AC-16
	17		AC-17	Access Control	AC-17
	18		AC-18	Access Control	AC-18
	19		AC-19	Access Control	AC-19
	20		AC-20	Access Control	AC-20
	21		AC-21	Access Control	AC-21
	22		AC-22	Access Control	AC-22
	00		AT-00	Awareness and Training	Awareness and Training Control Group
	01		AT-01	Awareness and Training	AT-01
	02		AT-02	Awareness and Training	AT-02
	03		AT-03	Awareness and Training	AT-03
	04		AT-04	Awareness and Training	AT-04
	05		AT-05	Awareness and Training	AT-05
	00		AU-00	Audit and Accountability	Audit and Accountability Control Group
	01		AU-01	Audit and Accountability	AU-01
	02		AU-02	Audit and Accountability	AU-02
	03		AU-03	Audit and Accountability	AU-03
	04		AU-04	Audit and Accountability	AU-04
	05		AU-05	Audit and Accountability	AU-05
	06		AU-06	Audit and Accountability	AU-06

	07		AU-07	Audit and Accountability	AU-07
	08		AU-08	Audit and Accountability	AU-08
	09		AU-09	Audit and Accountability	AU-09
	10		AU-10	Audit and Accountability	AU-10
	11		AU-11	Audit and Accountability	AU-11
	12		AU-12	Audit and Accountability	AU-12
	13		AU-13	Audit and Accountability	AU-13
	14		AU-14	Audit and Accountability	AU-14
	00		CA-00	Security Assessment and Authorization	Security Assessment and Authorization Control Group
	01		CA-01	Security Assessment and Authorization	CA-01
	02		CA-02	Security Assessment and Authorization	CA-02
	03		CA-03	Security Assessment and Authorization	CA-03
	04		CA-04	Security Assessment and Authorization	CA-04
	05		CA-05	Security Assessment and Authorization	CA-05
	06		CA-06	Security Assessment and Authorization	CA-06
	07		CA-07	Security Assessment and Authorization	CA-07
	00		CM-00	Configuration Management	Configuration Management Control Group
	01		CM-01	Configuration Management	CM-01
	02		CM-02	Configuration Management	CM-02
	03		CM-03	Configuration Management	CM-03
	04		CM-04	Configuration Management	CM-04
	05		CM-05	Configuration Management	CM-05
	06		CM-06	Configuration Management	CM-06
	07		CM-07	Configuration Management	CM-07
	08		CM-08	Configuration Management	CM-08
	09		CM-09	Configuration Management	CM-09
	00		CP-00	Contingency Planning	Contingency Planning Control Group
	01		CP-01	Contingency Planning	CP-01
	02		CP-02	Contingency Planning	CP-02
	03		CP-03	Contingency Planning	CP-03
	04		CP-04	Contingency Planning	CP-04
	05		CP-05	Contingency Planning	CP-05
	06		CP-06	Contingency Planning	CP-06
	07		CP-07	Contingency Planning	CP-07
	08		CP-08	Contingency Planning	CP-08

	09		CP-09	Contingency Planning	CP-09
	10		CP-10	Contingency Planning	CP-10
	00		IA-00	Identification and Authentication	Identification and Authentication Control Group
	01		IA-01	Identification and Authentication	IA-01
	02		IA-02	Identification and Authentication	IA-02
	03		IA-03	Identification and Authentication	IA-03
	04		IA-04	Identification and Authentication	IA-04
	05		IA-05	Identification and Authentication	IA-05
	06		IA-06	Identification and Authentication	IA-06
	07		IA-07	Identification and Authentication	IA-07
	08		IA-08	Identification and Authentication	IA-08
	00		IR-00	Incident Response	Incident Response Control Group
	01		IR-01	Incident Response	IR-01
	02		IR-02	Incident Response	IR-02
	03		IR-03	Incident Response	IR-03
	04		IR-04	Incident Response	IR-04
	05		IR-05	Incident Response	IR-05
	06		IR-06	Incident Response	IR-06
	07		IR-07	Incident Response	IR-07
	08		IR-08	Incident Response	IR-08
	00		MA-00	Maintenance	Maintenance Control Group
	01		MA-01	Maintenance	MA-01
	02		MA-02	Maintenance	MA-02
	03		MA-03	Maintenance	MA-03
	04		MA-04	Maintenance	MA-04
	05		MA-05	Maintenance	MA-05
	06		MA-06	Maintenance	MA-06
	00		MP-00	Media Protection	Media Protection Control Group
	01		MP-01	Media Protection	MP-01
	02		MP-02	Media Protection	MP-02
	03		MP-03	Media Protection	MP-03
	04		MP-04	Media Protection	MP-04

	05		MP-05	Media Protection	MP-05
	06		MP-06	Media Protection	MP-06
	00		PE-00	Physical and Environmental Protection	Physical and Environmental Protection Control Group
	01		PE-01	Physical and Environmental Protection	PE-01
	02		PE-02	Physical and Environmental Protection	PE-02
	03		PE-03	Physical and Environmental Protection	PE-03
	04		PE-04	Physical and Environmental Protection	PE-04
	05		PE-05	Physical and Environmental Protection	PE-05
	06		PE-06	Physical and Environmental Protection	PE-06
	07		PE-07	Physical and Environmental Protection	PE-07
	08		PE-08	Physical and Environmental Protection	PE-08
	09		PE-09	Physical and Environmental Protection	PE-09
	10		PE-10	Physical and Environmental Protection	PE-10
	11		PE-11	Physical and Environmental Protection	PE-11
	12		PE-12	Physical and Environmental Protection	PE-12
	13		PE-13	Physical and Environmental Protection	PE-13
	14		PE-14	Physical and Environmental Protection	PE-14
	15		PE-15	Physical and Environmental Protection	PE-15
	16		PE-16	Physical and Environmental Protection	PE-16
	17		PE-17	Physical and Environmental Protection	PE-17
	18		PE-18	Physical and Environmental Protection	PE-18
	19		PE-19	Physical and Environmental Protection	PE-19
	00		PL-00	Planning	Planning Control Group
	01		PL-01	Planning	PL-01
	02		PL-02	Planning	PL-02

	03		PL-03	Planning	PL-03
	04		PL-04	Planning	PL-04
	05		PL-05	Planning	PL-05
	06		PL-06	Planning	PL-06
	00		PS-00	Personnel Security	Personnel Security Control Group
	01		PS-01	Personnel Security	PS-01
	02		PS-02	Personnel Security	PS-02
	03		PS-03	Personnel Security	PS-03
	04		PS-04	Personnel Security	PS-04
	05		PS-05	Personnel Security	PS-05
	06		PS-06	Personnel Security	PS-06
	07		PS-07	Personnel Security	PS-07
	08		PS-08	Personnel Security	PS-08
	00		RA-00	Risk Assessment	Risk Assessment Control Group
	01		RA-01	Risk Assessment	RA-01
	02		RA-02	Risk Assessment	RA-02
	03		RA-03	Risk Assessment	RA-03
	04		RA-04	Risk Assessment	RA-04
	05		RA-05	Risk Assessment	RA-05
	00		SA-00	System and Services Acquisition	System and Services Acquisition Control Group
	01		SA-01	System and Services Acquisition	SA-01
	02		SA-02	System and Services Acquisition	SA-02
	03		SA-03	System and Services Acquisition	SA-03
	04		SA-04	System and Services Acquisition	SA-04
	05		SA-05	System and Services Acquisition	SA-05
	06		SA-06	System and Services Acquisition	SA-06
	07		SA-07	System and Services Acquisition	SA-07
	08		SA-08	System and Services Acquisition	SA-08
	09		SA-09	System and Services Acquisition	SA-09
	10		SA-10	System and Services Acquisition	SA-10
	11		SA-11	System and Services Acquisition	SA-11

	12		SA-12	System and Services Acquisition	SA-12
	13		SA-13	System and Services Acquisition	SA-13
	14		SA-14	System and Services Acquisition	SA-14
	00		SC-00	System and Communications Protection	System and Communications Protection Control Group
	01		SC-01	System and Communications Protection	SC-01
	02		SC-02	System and Communications Protection	SC-02
	03		SC-03	System and Communications Protection	SC-03
	04		SC-04	System and Communications Protection	SC-04
	05		SC-05	System and Communications Protection	SC-05
	06		SC-06	System and Communications Protection	SC-06
	07		SC-07	System and Communications Protection	SC-07
	08		SC-08	System and Communications Protection	SC-08
	09		SC-09	System and Communications Protection	SC-09
	10		SC-10	System and Communications Protection	SC-10
	11		SC-11	System and Communications Protection	SC-11
	12		SC-12	System and Communications Protection	SC-12
	13		SC-13	System and Communications Protection	SC-13
	14		SC-14	System and Communications Protection	SC-14
	15		SC-15	System and Communications Protection	SC-15
	16		SC-16	System and Communications Protection	SC-16
	17		SC-17	System and Communications Protection	SC-17
	18		SC-18	System and Communications Protection	SC-18

	19		SC-19	System and Communications Protection	SC-19
	20		SC-20	System and Communications Protection	SC-20
	21		SC-21	System and Communications Protection	SC-21
	22		SC-22	System and Communications Protection	SC-22
	23		SC-23	System and Communications Protection	SC-23
	24		SC-24	System and Communications Protection	SC-24
	25		SC-25	System and Communications Protection	SC-25
	26		SC-26	System and Communications Protection	SC-26
	27		SC-27	System and Communications Protection	SC-27
	28		SC-28	System and Communications Protection	SC-28
	29		SC-29	System and Communications Protection	SC-29
	30		SC-30	System and Communications Protection	SC-30
	31		SC-31	System and Communications Protection	SC-31
	32		SC-32	System and Communications Protection	SC-32
	33		SC-33	System and Communications Protection	SC-33
	34		SC-34	System and Communications Protection	SC-34
	00		SI-00	System and Information Integrity	System and Information Integrity Control Group
	01		SI-01	System and Information Integrity	SI-01
	02		SI-02	System and Information Integrity	SI-02
	03		SI-03	System and Information Integrity	SI-03
	04		SI-04	System and Information Integrity	SI-04
	05		SI-05	System and Information Integrity	SI-05

	06		SI-06	System and Information Integrity	SI-06
	07		SI-07	System and Information Integrity	SI-07
	08		SI-08	System and Information Integrity	SI-08
	09		SI-09	System and Information Integrity	SI-09
	10		SI-10	System and Information Integrity	SI-10
	11		SI-11	System and Information Integrity	SI-11
	12		SI-12	System and Information Integrity	SI-12
	13		SI-13	System and Information Integrity	SI-13
	00		PM-00	Program Management	Program Management Control Group
	01		PM-01	Program Management	PM-01
	02		PM-02	Program Management	PM-02
	03		PM-03	Program Management	PM-03
	04		PM-04	Program Management	PM-04
	05		PM-05	Program Management	PM-05
	06		PM-06	Program Management	PM-06
	07		PM-07	Program Management	PM-07
	08		PM-08	Program Management	PM-08
	09		PM-09	Program Management	PM-09
	10		PM-10	Program Management	PM-10
	11		PM-11	Program Management	PM-11

V Consolidated Non-Functional Requirements
ceability Matrix (RTM)
T 800 Series

Requirement Description	Requirement Fulfilled?	Notes	Evidence
ing Provider can meet all Access Control measures in the Access Control Group			
ss Control Policy and Procedures	Y		
unt Management	Y		
ss Enforcement	Y		
rmation Flow Enforcement	Y		
ration of Duties	Y		
t Privilege	Y		
uccessful Login Attempts	Y		
em Use Notification	Y		
ious Logon (Access) Notification	Y		
current Session Control	Y		
ion Lock	Y		
ion Termination (Withdrawn)	Y		
ervision and Review—Access Control (Withdrawn)	Y		
nitted Actions without Identification or Authentication	Y		
omated Marking (Withdrawn)	Y		
rity Attributes	Y		
ote Access	Y		
eless Access	Y		
ss Control for Mobile Devices	Y		
of External Information Systems	Y		
-Based Collaboration and Information Sharing	Y		
icly Accessible Content	Y		
ing Provider can meet all Awareness and Training measures in the Awareness and ning Control Group			
rity Awareness and Training Policy and Procedures	Y		
rity Awareness	Y		
rity Training	Y		
rity Training Records	Y		
acts with Security Groups and Associations	Y		
ing Provider can meet all Audit and Accountability measures in the Audit and ountability Control Group.			
t and Accountability Policy and Procedures .	Y		
table Events	Y		
ent of Audit Records	Y		
t Storage Capacity	Y		
onse to Audit Processing Failures	Y		
t Review, Analysis, and Reporting	Y		

t Reduction and Report Generation	Y		
Stamps	Y		
ection of Audit Information	Y		
repudiation	Y		
t Record Retention	Y		
t Generation	Y		
itoring for Information Disclosure	Y		
on Audit	Y		
ng Provider can meet all Security Assessment and Authorization measures in the rity Assessment and Authorization Control Group			
rity Assessment and Authorization Policies and Procedures	Y		
rity Assessments	Y		
mation System Connections	Y		
rity Certification (Withdrawn)	Y		
of Action and Milestones	Y		
rity Authorization	Y		
inuous Monitoring	Y		
ng Provider can meet all Configuration Management measures in the guration Management Control Group			
guration Management Policy and Procedures	Y		
ine Configuration	Y		
guration Change Control	Y		
rity Impact Analysis	Y		
ss Restrictions for Change	Y		
guration Settings	Y		
Functionality	Y		
mation System Component Inventory	Y		
guration Management Plan	Y		
ng Provider can meet all Contingency Planning measures in the Contingency ning Control Group			
ngency Planning Policy and Procedures	Y		
ngency Plan	Y		
ngency Training	Y		
ngency Plan Testing and Exercises	Y		
ngency Plan Update (Withdrawn)	Y		
nate Storage Site	Y		
nate Processing Site	Y		
ommunications Services	Y		

ormation System Backup	Y		
ormation System Recovery and Reconstitution	Y		
tion Provider can meet all Identification and Authentication measures in the Identification and Authentication Control Group			
ntification and Authentication Policy and Procedures	Y		
ntification and Authentication (Organizational Users)	Y		
vice Identification and Authentication	Y		
ntifier Management	Y		
henticator Management	Y		
henticator Feedback	Y		
ptographic Module Authentication	Y		
ntification and Authentication (Non-Organizational Users)	Y		
ting Provider can meet all Incident Response measures in the Incident Response Control Group			
dent Response Policy and Procedures	Y		
dent Response Training	Y		
dent Response Testing and Exercises	Y		
dent Handling	Y		
dent Monitoring	Y		
dent Reporting	Y		
dent Response Assistance	Y		
dent Response Plan	Y		
ting Provider can meet all Maintenance measures in the Maintenance Control Group			
tem Maintenance Policy and Procedures	Y		
ntrolled Maintenance	Y		
intenance Tools	Y		
n-Local Maintenance	Y		
intenance Personnel	Y		
ely Maintenance	Y		
tion Provider can meet all Media Protection measures in the Media Protection Control Group			
dia Protection Policy and Procedures			
dia Access	Y		
dia Marking	Y		
dia Storage	Y		

dia Transport	Y		
dia Sanitization	Y		
sting Provider can meet all Physical and Environmental Protection measures in the ysical and Environmental Protection Control Group			
ysical and Environmental Protection Policy and Procedures	Y		
ysical Access Authorizations	Y		
ysical Access Control	Y		
cess Control for Transmission Medium	Y		
cess Control for Output Devices	Y		
nitoring Physical Access	Y		
tor Control	Y		
ess Records	Y		
ver Equipment and Power Cabling	Y		
ergency Shutoff	Y		
ergency Power	Y		
ergency Lighting	Y		
Protection	Y		
nperature and Humidity Controls	Y		
ter Damage Protection	Y		
ivery and Removal	Y		
ernate Work Site	Y		
ation of Information System Components	Y		
rmation Leakage	Y		
ting Provider can meet all Planning measures in the Planning Control Group			
urity Planning Policy and Procedures	Y		
tem Security Plan	Y		

ystem Security Plan Update (Withdrawn)	Y		
ules of Behavior	Y		
rivacy Impact Assessment	Y		
ecurity-Related Activity Planning	Y		
osting Provider can meet all Personnel Security measures in the Personnel Security ontrol Group			
ersonnel Security Policy and Procedures	Y		
osition Categorization	Y		
ersonnel Screening	Y		
ersonnel Termination	Y		
ersonnel Transfer	Y		
ccess Agreements	Y		
hird-Party Personnel Security	Y		
ersonnel Sanctions	Y		
osting Provider can meet all Risk Assessment measures in the Risk Assessment ontrol Group			
sk Assessment Policy and Procedures	Y		
ecurity Categorization	Y		
sk Assessment	Y		
sk Assessment Update (Withdrawn)	Y		
ulnerability Scanning	Y		
osting Provider can meet all System and Services Acquisition measures in the System nd Services Acquisition Control Group			
ystem and Services Acquisition Policy and Procedures	Y		
llocation of Resources	Y		
fe Cycle Support	Y		
cquisitions	Y		
formation System Documentation	Y		
oftware Usage Restrictions	Y		
ser-Installed Software	Y		
ecurity Engineering Principles	Y		
xternal Information System Services	Y		
eveloper Configuration Management	Y		
eveloper Security Testing	Y		

pply Chain Protection	Y		
stworthiness	Y		
tical Information System Components	Y		
ting Provider can meet all System and Communications Protection measures in the tem and Communications Protection Control Group			
tem and Communications Protection Policy and Procedures	Y		
plication Partitioning	Y		
urity Function Isolation	Y		
ormation in Shared Resources	Y		
nial of Service Protection	Y		
ource Priority	Y		
ndary Protection	Y		
nsmission Integrity	Y		
nsmission Confidentiality	Y		
work Disconnect	Y		
sted Path	Y		
ptographic Key Establishment and Management	Y		
of Cryptography	Y		
lic Access Protections	Y		
aborative Computing Devices	Y		
nsmission of Security Attributes	Y		
lic Key Infrastructure Certificates	Y		
pile Code	Y		

oice Over Internet Protocol	Y		
ecure Name /Address Resolution Service uthoritative Source)	Y		
ecure Name /Address Resolution Service ecursive or Caching Resolver)	Y		
rchitecture and Provisioning for ame/Address Resolution Service	Y		
ession Authenticity	Y		
il in Known State	Y		
ain Nodes	Y		
oneypots	Y		
perating System-Independent Applications	Y		
rotection of Information at Rest	Y		
eterogeneity	Y		
rtualization Techniques	Y		
overt Channel Analysis	Y		
formation System Partitioning	Y		
ransmission Preparation Integrity	Y		
on-Modifiable Executable Programs	Y		
osting Provider can meet all System and Information Integrity measures in the stem and Information Integrity Control Group			
ystem and Information Integrity Policy and Procedures	Y		
aw Remediation	Y		
alicious Code Protection	Y		
formation System Monitoring	Y		
ecurity Alerts, Advisories, and Directives	Y		

ty Functionality Verification	Y		
are and Information Integrity	Y		
Protection	Y		
ation Input Restrictions	Y		
ation Input Validation	Y		
Handling	Y		
ation Output Handling and Retention	Y		
table Failure Prevention	Y		
g Provider can meet all Program Management measures in the Program gement Control Group			
ation Security Program Plan	Y		
Information Security Officer	Y		
ation Security Resources	Y		
f Action and Milestones Process	Y		
ation System Inventory	Y		
ation Security Measures of Performance	Y		
rise Architecture	Y		
l Infrastructure Plan	Y		
lanagement Strategy	Y		
ty Authorization Process	Y		
n/Business Process Definition	Y		

Level	Sub	Req ID-New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
		AC-01.00-00	AC-01 ACCESS CONTROL POLICY AND PROCEDURES	AC-01.00-00	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:			
		AC-01.01-01	AC-01 ACCESS CONTROL POLICY AND PROCEDURES	AC-01.01-01	a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		AC-01.01-02	AC-01 ACCESS CONTROL POLICY AND PROCEDURES	AC-01.01-02	b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	Y		
			AC-01 ACCESS CONTROL POLICY AND PROCEDURES	Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and	Y		
		AC-02.01-00	AC-02 ACCOUNT MANAGEMENT	AC-02.01-00	Control: The organization manages information system accounts, including:	Y		
		AC-02.01-01	AC-02 ACCOUNT MANAGEMENT	AC-02.01-01	a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);	Y		
		AC-02.01-02	AC-02 ACCOUNT MANAGEMENT	AC-02.01-02	b. Establishing conditions for group membership;	Y		
		AC-02.01-03	AC-02 ACCOUNT MANAGEMENT	AC-02.01-03	c. Identifying authorized users of the information system and specifying access privileges;	Y		
		AC-02.01-04	AC-02 ACCOUNT MANAGEMENT	AC-02.01-04	d. Requiring appropriate approvals for requests to establish accounts;	Y		
		AC-02.01-05	AC-02 ACCOUNT MANAGEMENT	AC-02.01-05	e. Establishing, activating, modifying, disabling, and removing accounts;	Y		
		AC-02.01-06	AC-02 ACCOUNT MANAGEMENT	AC-02.01-06	f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;	Y		
		AC-02.01-07	AC-02 ACCOUNT MANAGEMENT	AC-02.01-07	g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;	Y		
		AC-02.01-08	AC-02 ACCOUNT MANAGEMENT	AC-02.01-08	h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;	Y		
		AC-02.01-09	AC-02 ACCOUNT MANAGEMENT	AC-02.01-09	i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and	Y		
		AC-02.01-10	AC-02 ACCOUNT MANAGEMENT	AC-02.01-10	j. Reviewing accounts [*Assignment: organization-defined frequency*].	Y		
			AC-02 ACCOUNT MANAGEMENT	Supplemental Guidance	Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for	Y		
		AC-02(1).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(1).01-00	(1) The organization employs automated mechanisms to support the management of information system accounts.	Y		
		AC-02(2).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(2).01-00	(2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].	Y		
		AC-02(3).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(3).01-00	(3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].	Y		
		AC-02(4).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(4).01-00	(4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	Y		
		AC-02(5).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-00	(5) The organization:	Y		
		AC-02(5).01-01	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-01	(a) Requires that users log out when [*Assignment: organization defined time-period of expected inactivity and/or description of when to log out*];	Y		
		AC-02(5).01-02	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-02	(b) Determines normal time-of-day and duration usage for information system accounts;	Y		
		AC-02(5).01-03	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-03	(c) Monitors for atypical usage of information system accounts; and	Y		
		AC-02(5).01-04	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-04	(d) Reports atypical usage to designated organizational officials.	Y		
		AC-02(6).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(6).01-00	(6) The information system dynamically manages user privileges and associated access authorizations.	Y		
			AC-02 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, many service-oriented architecture implementations rely on run time access control decisions facilitated by dynamic privilege management. While user identities remain	Y		
		AC-02(7).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(7).01-00	(7) The organization:	Y		
		AC-02(7).01-01	AC-02 CONTROL ENHANCEMENTS	AC-02(7).01-01	(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and	Y		
		AC-02(7).01-02	AC-02 CONTROL ENHANCEMENTS	AC-02(7).01-02	(b) Tracks and monitors privileged role assignments.	Y		
		AC-03.01-00	AC-03 ACCESS ENFORCEMENT	AC-03.01-00	Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	Y		
			AC-03 CONTROL ENHANCEMENTS	Supplemental Guidance	Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files,	Y		
		AC-03(1).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(1).01-00	(1) [Withdrawn: Incorporated into AC-6].	Y		
		AC-03(2).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(2).01-00	(2) The information system enforces dual authorization, based on organizational policies and procedures for [*Assignment: organization-defined privileged commands*].	Y		
			AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Dual authorization mechanisms require two forms of approval to execute. The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.	Y		
		AC-03(3).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(3).01-00	(3) The information system enforces [*Assignment: organization-defined nondiscretionary access control policies*] over [*Assignment: organization-defined set of users and resources*] where the policy rule set for each policy specifies:	Y		

	AC-03(3).01-01	AC-03 CONTROL ENHANCEMENTS	AC-03(3).01-01	(a) Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and	Y		
	AC-03(3).01-02	AC-03 CONTROL ENHANCEMENTS	AC-03(3).01-02	(b) Required relationships among the access control information to permit access.	Y		
		AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, Mandatory Access Control, and Originator Controlled Access Control. Nondiscretionary access control policies may be employed by organizations in addition to the employment of	Y		
	--	AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	*For Role-Based Access Control (RBAC):* Policy establishes coverage over all users and resources to ensure that access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role.	Y		
	AC-03(4).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-00	(4) The information system enforces a Discretionary Access Control (DAC) policy that:	Y		
	AC-03(4).01-01	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-01	(a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both;	Y		
	AC-03(4).01-02	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-02	(b) Limits propagation of access rights; and	Y		
	AC-03(4).01-03	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-03	(c) Includes or excludes access to the granularity of a single user.	Y		
	AC-03(5).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(5).01-00	(5) The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, nonoperable system states.	Y		
		AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Security-relevant information is any information within the information system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Filtering rules for routers and firewalls, cryptographic	Y		
	AC-03(6).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(6).01-00	(6) The organization encrypts or stores off-line in a secure location [*Assignment: organization-defined user and/or system information*].	Y		
		AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The use of encryption by the organization reduces the probability of unauthorized disclosure of information and can also detect unauthorized changes to information. Removing information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access via a	Y		
	AC-04.01-00	AC-4 INFORMATION FLOW ENFORCEMENT	AC-04.01-00	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Y		
			Supplemental Guidance	Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping	Y		
	AC-04(1).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(1).01-00	(1) The information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions.	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Information flow enforcement mechanisms compare security attributes on all information (data content and data structure), source and destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by the	Y		
	AC-04(2).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(2).01-00	(2) The information system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.	Y		
	AC-04(3).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(3).01-00	(3) The information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.	Y		
	AC-04(4).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(4).01-00	(4) The information system prevents encrypted data from bypassing content-checking mechanisms.	Y		
	AC-04(5).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(5).01-00	(5) The information system enforces [*Assignment: organization-defined limitations on the embedding of data types within other data types*].	Y		
	AC-04(6).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(6).01-00	(6) The information system enforces information flow control on metadata.	Y		
	AC-04(7).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(7).01-00	(7) The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.	Y		
	AC-04(8).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(8).01-00	(8) The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions.	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Organization-defined security policy filters include, for example, dirty word filters, file type checking filters, structured data filters, unstructured data filters, metadata content filters, and hidden content filters. Structured data permits the interpretation of its content by virtue of atomic elements that are	Y		
	AC-04(9).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(9).01-00	(9) The information system enforces the use of human review for [*Assignment: organization-defined security policy filters*] when the system is not capable of making an information flow control decision.	Y		
	AC-04(10).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(10).01-00	(10) The information system provides the capability for a privileged administrator to enable/disable [*Assignment: organization-defined security policy filters*].	Y		
	AC-04(11).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(11).01-00	(11) The information system provides the capability for a privileged administrator to configure [*Assignment: organization-defined security policy filters*] to support different security policies.	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: For example, to reflect changes in the security policy, an administrator can change the list of "dirty words" that the security policy mechanism checks in accordance with the definitions provided by the organization.	Y		
	AC-04(12).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(12).01-00	(12) The information system, when transferring information between different security domains, identifies information flows by data type specification and usage.	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Data type specification and usage include, for example, using file naming to reflect type of data and limiting data transfer based on file type.	Y		
	AC-04(13).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(13).01-00	(13) The information system, when transferring information between different security domains, decomposes information into policy-relevant subcomponents for submission to policy enforcement mechanisms.	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Policy enforcement mechanisms include the filtering and/or sanitization rules that are applied to information prior to transfer to a different security domain. Parsing transfer files facilitates policy decisions on source, destination, certificates, classification, subject, attachments, and other information security-related	Y		
	AC-04(14).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(14).01-00	(14) The information system, when transferring information between different security domains, implements policy filters that constrain data structure and content to [*Assignment: organization-defined information security policy requirements*].	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Constraining file lengths, allowed enumerations, character sets, schemas, and other data object attributes reduces the range of potential malicious and/or unsanctioned content. Examples of constraints include ensuring that: (i) character data fields only contain printable ASCII; (ii) character data fields only contain	Y		
	AC-04(15).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(15).01-00	(15) The information system, when transferring information between different security domains, detects unsanctioned information and prohibits the transfer of such information in accordance with the security policy.	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Actions to support this enhancement include: checking all transferred information for malware, implementing dirty word list searches on transferred information, and applying the same protection measures to metadata (e.g., security attributes) that is applied to the information payload.	Y		
	AC-04(16).01-00	Control Enhancements:	AC-04(16).01-00	(16) The information system enforces security policies regarding information on interconnected systems.	Y		
		AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Transferring information between interconnected information systems of differing security policies introduces risk that such transfers violate one or more policies. While security policy violations may not be absolutely prohibited, policy guidance from information owners/stewards is implemented at the policy	Y		
	AC-04(17).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-00	(17) The information system:	Y		

		AC-04(17).01-01	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-01	(a) Uniquely identifies and authenticates source and destination domains for information transfer;	Y		
		AC-04(17).01-02	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-02	(b) Binds security attributes to information to facilitate information flow policy enforcement; and	Y		
		AC-04(17).01-03	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-03	(c) Tracks problems associated with the security attribute binding and information transfer.	Y		
			AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in an information system, allows forensic reconstruction of events when required, and increases policy compliance by attributing policy violations to specific	Y		
		AC-05.01-00	AC-05 SEPARATION OF DUTIES	AC-05.01-00	Control: The organization:	Y		
		AC-05.01-01	AC-05 SEPARATION OF DUTIES	AC-05.01-01	a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;	Y		
		AC-05.01-02	AC-05 SEPARATION OF DUTIES	AC-05.01-02	b. Documents separation of duties; and	Y		
		AC-05.01-03	AC-05 SEPARATION OF DUTIES	AC-05.01-03	c. Implements separation of duties through assigned information system access authorizations.	Y		
			AC-05 SEPARATION OF DUTIES	Supplemental Guidance	Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systemsprogramming, configuration management, quality	Y		
		AC-06.01-00	AC-06 LEAST PRIVILEGE	AC-06.01-00	Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Y		
			AC-06 LEAST PRIVILEGE	Supplemental Guidance	Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to	Y		
		AC-06(1).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(1).01-00	(1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*].	Y		
			AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network	Y		
		AC-06(2).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(2).01-00	(2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	Y		
			AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of *role* is intended to address those situations where an access control policy such as *Role Based Access Control (RBAC)* is being implemented and where a change of role provides the same	Y		
		AC-06(3).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(3).01-00	(3) The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	Y		
		AC-06(4).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(4).01-00	(4) The information system provides separate processing domains to enable finer-grained allocation of user privileges.	Y		
			AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Employing virtualization techniques to allow greater privilege within a virtual machine while restricting privilege to the underlying actual machine is an example of providing separate processing domains for finer-grained allocation of user privileges.	Y		
		AC-06(5).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(5).01-00	(5) The organization limits authorization to super user accounts on the information system to designated system administration personnel.	Y		
			AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Super user accounts are typically described as "root" or "administrator" for various types of commercial off-the-shelf operating systems. Configuring organizational information systems (e.g., notebook/laptop computers, servers, workstations) such that day-to-day users are not authorized access to super user	Y		
		AC-06(6).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(6).01-00	(6) The organization prohibits privileged access to the information system by non-organizational users.	Y		
			AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: A qualified organizational user may be advised by a non-organizational user, if necessary.	Y		
		AC-07.01-00	AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	AC-07.01-00	Control: The information system:	Y		
		AC-07.01-01	AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	AC-07.01-01	a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and	Y		
		AC-07.01-02	AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	AC-07.01-02	b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless	Y		
			AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	Supplemental Guidance	Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information	Y		
		AC-07(1).01-00	AC-07 CONTROL ENHANCEMENTS	AC-07(1).01-00	(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	Y		
		AC-07(2).01-00	AC-07 CONTROL ENHANCEMENTS	AC-07(2).01-00	(2) The information system provides additional protection for mobile devices accessed via login by purging information from the device after [*Assignment: organization-defined number*] consecutive, unsuccessful login attempts to the device.	Y		
			AC-07 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This enhancement applies only to mobile devices for which a login occurs (e.g., personal digital assistants) and not to mobile devices accessed without a login such as removable media. In certain situations, this enhancement may not apply to mobile devices if the information on the device is encrypted with	Y		
		AC-08.01-00	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-00	Control: The information system:	Y		
		AC-08.01-01	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-01	a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system	Y		
		AC-08.01-02	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-02	b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and	Y		
		AC-08.01-03	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-03	c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the	Y		
			AC-08 SYSTEM USE NOTIFICATION	Supplemental Guidance	Supplemental Guidance: System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an	Y		
		AC-09.01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09.01-00	Control: The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).	Y		
			AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	Supplemental Guidance	Supplemental Guidance: This control is intended to cover both traditional logons to information systems and general accesses to information systems that occur in other types of architectural configurations (e.g., service oriented architectures).	Y		
		AC-09(1).01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09(1).01-00	(1) The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.	Y		
		AC-09(2).01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09(2).01-00	(2) The information system notifies the user of the number of [*Selection: successful logins/accesses; unsuccessful login/access attempts; both*] during [*Assignment: organization-defined time period*].	Y		
		AC-09(3).01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09(3).01-00	(3) The information system notifies the user of [*Assignment: organization-defined set of security-related changes to the user's account*] during [*Assignment: organization-defined time period*].	Y		

		AC-10.01-00	AC-10 CONCURRENT SESSION CONTROL	AC-10.01-00	Control: The information system limits the number of concurrent sessions for each system account to [*Assignment: organization-defined number*].	Y		
			AC-10 CONCURRENT SESSION CONTROL	Supplemental Guidance	Supplemental Guidance: The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system	Y		
		AC-11.01-00	AC-11 SESSION LOCK	AC-11.01-00	Control: The information system:	Y		
		AC-11.01-01	AC-11 SESSION LOCK	AC-11.01-01	a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and	Y		
		AC-11.01-02	AC-11 SESSION LOCK	AC-11.01-02	b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Y		
			AC-11 SESSION LOCK	Supplemental Guidance	Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically	Y		
		AC-11(1).01-00	AC-11 CONTROL ENHANCEMENTS	AC-11(1).01-00	(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.	Y		
		AC-12.01-00	AC-12 SESSION TERMINATION	AC-12.01-00	[Withdrawn: Incorporated into SC-10].	Y		
		AC-13.01-00	AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL	AC-13.01-00	[Withdrawn: Incorporated into AC-2 and AU-6].	Y		
		AC-14.01-00	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14.01-00	Control: The organization:	Y		
		AC-14.01-01	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14.01-01	a. Identifies specific user actions that can be performed on the information system without identification or authentication; and	Y		
		AC-14.01-02	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14.01-02	b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	Y		
			AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	Supplemental Guidance	Supplemental Guidance: This control is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication	Y		
		AC-14(1).01-00	AC-14 CONTROL ENHANCEMENTS	AC-14(1).01-00	(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	Y		
		AC-15.01-00	AC-15 AUTOMATED MARKING	AC-15.01-00	[Withdrawn: Incorporated into MP-3].	Y		
		AC-16.01-00	AC-16 SECURITY ATTRIBUTES	AC-16.01-00	Control: The information system supports and maintains the binding of [*Assignment: organization-defined security attributes*] to information in storage, in process, and in transmission.	Y		
			AC-16 SECURITY ATTRIBUTES	Supplemental Guidance	Supplemental Guidance: Security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information. These attributes are typically associated with internal data structures (e.g., records, buffers, files) within the information system and are used to enable	Y		
		AC-16(1).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(1).01-00	(1) The information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.	Y		
		AC-16(2).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(2).01-00	(2) The information system allows authorized entities to change security attributes.	Y		
		AC-16(3).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(3).01-00	(3) The information system maintains the binding of security attributes to information with sufficient assurance that the information--attribute association can be used as the basis for automated policy actions.	Y		
			AC-16 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhanced Supplemental Guidance: Examples of automated policy actions include automated access control decisions (e.g., Mandatory Access Control decisions), or decisions to release (or not release) information (e.g., information flows via cross domain systems).	Y		
		AC-16(4).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(4).01-00	(4) The information system allows authorized users to associate security attributes with information.	Y		
			AC-16 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhanced Supplemental Guidance: The support provided by the information system can vary from prompting users to select security attributes to be associated with specific information objects, to ensuring that the combination of attributes selected is valid.	Y		
		AC-16(5).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(5).01-00	(5) The information system displays security attributes in human-readable form on each object output from the system to system output devices to identify [*Assignment: organization-identified set of special dissemination, handling, or distribution instructions*] using [*Assignment: organization-identified human readable, standard naming*	Y		
			AC-16 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Objects output from the information system include, for example, pages, screens, or equivalent. Output devices include, for example, printers and video displays on computer terminals, monitors, screens on notebook/laptop computers and personal digital assistants.	Y		
		AC-17.01-00	AC-17 REMOTE ACCESS	AC-17.01-00	Control: The organization:	Y		
		AC-17.01-01	AC-17 REMOTE ACCESS	AC-17.01-01	a. Documents allowed methods of remote access to the information system;	Y		
		AC-17.01-02	AC-17 REMOTE ACCESS	AC-17.01-02	b. Establishes usage restrictions and implementation guidance for each allowed remote access method;	Y		
		AC-17.01-03	AC-17 REMOTE ACCESS	AC-17.01-03	c. Monitors for unauthorized remote access to the information system;	Y		
		AC-17.01-04	AC-17 REMOTE ACCESS	AC-17.01-04	d. Authorizes remote access to the information system prior to connection; and	Y		
		AC-17.01-05	AC-17 REMOTE ACCESS	AC-17.01-05	e. Enforces requirements for remote connections to the information system.	Y		
			AC-17 REMOTE ACCESS	Supplemental Guidance	Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are	Y		
		AC-17(1).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(1).01-00	(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	Y		
			AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.	Y		
		AC-17(2).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(2).01-00	(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.	Y		
			AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13.	Y		
		AC-17(3).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(3).01-00	(3) The information system routes all remote accesses through a limited number of managed access control points.	Y		
			AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Related control: SC-7.	Y		
		AC-17(4).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(4).01-00	(4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	Y		

				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Related control: AC-6.	Y		
			AC-17(5).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(5).01-00	(5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.	Y		
			AC-17(6).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(6).01-00	(6) The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.	Y		
			AC-17(7).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(7).01-00	(7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited.	Y		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.	Y		
			AC-17(8).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(8).01-00	(8) The organization disables [*Assignment: organization-defined networking protocols within the information system deemed to be nonsecure*] except for explicitly identified components in support of specific operational requirements.	Y		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.	Y		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	Control: The organization:	Y		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	a. Establishes usage restrictions and implementation guidance for wireless access;	Y		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	b. Monitors for unauthorized wireless access to the information system;	Y		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	c. Authorizes wireless access to the information system prior to connection; and	Y		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	d. Enforces requirements for wireless connections to the information system.	Y		
				AC-18 WIRELESS ACCESS	Supplemental Guidance	Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the	Y		
			AC-18(1).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(1).01-00	(1) The information system protects wireless access to the system using authentication and encryption.	Y		
				AC-18 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary. Related control: SC-13.	Y		
			AC-18(2).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(2).01-00	(2) The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.	Y		
				AC-18 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed	Y		
			AC-18(3).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(3).01-00	(3) The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	Y		
			AC-18(4).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(4).01-00	(4) The organization does not allow users to independently configure wireless networking capabilities.	Y		
			AC-18(5).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(5).01-00	(5) The organization confines wireless communications to organization-controlled boundaries.	Y		
				AC-18 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Actions that may be taken by the organization to confine wireless communications to organization-controlled boundaries include: (i) reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the organization; (ii) employing measures such as TEMPEST to control wireless	Y		
			AC-19.01-00	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-00	Control: The organization:	Y		
			AC-19.01-01	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-01	a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;	Y		
			AC-19.01-02	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-02	b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;	Y		
			AC-19.01-03	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-03	c. Monitors for unauthorized connections of mobile devices to organizational information systems;	Y		
			AC-19.01-04	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-04	d. Enforces requirements for the connection of mobile	Y		
			AC-19.01-05	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-05	e. devices to organizational information systems;	Y		
			AC-19.01-06	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-06	f. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;	Y		
			AC-19.01-07	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-07	g. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and	Y		
			AC-19.01-08	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-08	h. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	Y		
				AC-19 ACCESS CONTROL FOR MOBILE DEVICES	Supplemental Guidance	Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-	Y		
				AC-19 ACCESS CONTROL FOR MOBILE DEVICES	Supplemental Guidance	Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the	Y		
			AC-19(1).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(1).01-00	(1) The organization restricts the use of writable, removable media in organizational information systems.	Y		
			AC-19(2).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(2).01-00	(2) The organization prohibits the use of personally owned, removable media in organizational information systems.	Y		
			AC-19(3).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(3).01-00	(3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.	Y		
				AC-19 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).	Y		
			AC-19(4).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(4).01-00	(4) The organization:	Y		
			AC-19(4).01-01	AC-19 CONTROL ENHANCEMENTS	AC-19(4).01-01	(a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing official(s); and	Y		
			AC-19(4).01-02	AC-19 CONTROL ENHANCEMENTS	AC-19(4).01-02	(b) Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:	Y		

		AC-20.01-00	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	AC-20.01-00	Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:	Y		
		AC-20.01-01	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	AC-20.01-01	a. Access the information system from the external information systems; and	Y		
		AC-20.01-02	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	AC-20.01-02	b. Process, store, and/or transmit organization-controlled information using the external information systems.	Y		
			AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	Enhanced Supplemental Guidance	This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational	Y		
		AC-20(1).01-00	AC-20 CONTROL ENHANCEMENTS	AC-20(1).01-00	(1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:	Y		
		AC-20(1).01-01	AC-20 CONTROL ENHANCEMENTS	AC-20(1).01-01	(a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or	Y		
		AC-20(1).01-02	AC-20 CONTROL ENHANCEMENTS	AC-20(1).01-02	(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.	Y		
		AC-20(2).01-00	AC-20 CONTROL ENHANCEMENTS	AC-20(2).01-00	(2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	Y		
			AC-20 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Limits on the use of organization-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.	Y		
		AC-21.01-00	AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING	AC-21.01-00	Control: The organization:	Y		
		AC-21.01-01	AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING	AC-21.01-01	a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and	Y		
		AC-21.01-02	AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING	AC-21.01-02	b. Employs [*Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required*] to assist users in making information sharing/collaboration decisions.	Y		
			AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING	Supplemental Guidance	Supplemental Guidance: The control applies to information that may be restricted in some manner (e.g., privileged medical, contract-sensitive, proprietary, personally identifiable information, special access programs/compartments) based on some formal or administrative determination. Depending on the information-sharing circumstance, the sharing	Y		
		AC-21(1).01-00	AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING	AC-21(1).01-00	(1) The information system employs automated mechanisms to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.	Y		
		AC-22.01-00	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-00	Control: The organization:	Y		
		AC-22.01-01	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-01	a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;	Y		
		AC-22.01-02	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-02	b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;	Y		
		AC-22.01-03	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-03	c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;	Y		
		AC-22.01-04	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-04	d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and	Y		
		AC-22.01-05	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-05	e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	Y		
			AC-22 PUBLICLY ACCESSIBLE CONTENT	Supplemental Guidance	Supplemental Guidance: Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information.	Y		
		AT-01.01-00	AT-01 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	AT-01.01-00	Control: The organization develops, disseminates, and reviews/updates: [*Assignment: organization-defined frequency*]:	Y		
		AT-01.01-01	AT-01 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	AT-01.01-01	a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		AT-01.01-02	AT-01 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	AT-01.01-02	b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	Y		
			AT-01 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies,	Y		
		AT-02.01-00	AT-02 SECURITY AWARENESS	AT-02.01-00	Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.	Y		
			AT-02 SECURITY AWARENESS	Supplemental Guidance	Supplemental Guidance: The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information	Y		
		AT-02(1).01-00	AT-02 CONTROL ENHANCEMENTS	AT-02(1).01-00	(1) The organization includes practical exercises in security awareness training that simulate actual cyber attacks.	Y		
			AT-02 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking malicious web links.	Y		
		AT-03.01-00	AT-03 SECURITY TRAINING	AT-03.01-00	Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.	Y		
			AT-03 SECURITY TRAINING	Supplemental Guidance	Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network	Y		
		AT-03.01-01	AT-03 SECURITY TRAINING	AT-03.01-01	(1) The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.	Y		
			AT-03 SECURITY TRAINING	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.	Y		
		AT-03.01-02	AT-03 SECURITY TRAINING	AT-03.01-02	(2) The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.	Y		
			AT-03 SECURITY TRAINING	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring and surveillance equipment, and security guards (deployment and operating procedures).	Y		
		AT-04.01-00	AT-04 SECURITY TRAINING RECORDS	AT-04.01-00	Control: The organization:	Y		
		AT-04.01-01	AT-04 SECURITY TRAINING RECORDS	AT-04.01-01	a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and	Y		
		AT-04.01-02	AT-04 SECURITY TRAINING RECORDS	AT-04.01-02	b. Retains individual training records for [*Assignment: organization-defined time period*].	Y		
			AT-04 SECURITY TRAINING RECORDS	Supplemental Guidance	Supplemental Guidance: While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.	Y		

		AT-05.01-00	AT-05 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	AT-05.01-00	Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:	Y		
			AT-05 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	Supplemental Guidance	Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security	Y		
		AU-01.00-00	AU-01 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	AU-01.01-00	Control: The organization develop, disseminate, and review/update [*Assignment: organization-defined frequency*]:	Y		
		AU-01.01-01	AU-01 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	AU-01.01-01	a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		AU-01.01-02	AU-01 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	AU-01.01-02	b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	Y		
			AU-01 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations,	Y		
		AU-02.01-00	AU-02 AUDITABLE EVENTS	AU-02.01-00	Control: The organization:	Y		
		AU-02.01-01	AU-02 AUDITABLE EVENTS	AU-02.01-01	a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*];	Y		
		AU-02.01-02	AU-02 AUDITABLE EVENTS	AU-02.01-02	b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;	Y		
		AU-02.01-03	AU-02 AUDITABLE EVENTS	AU-02.01-03	c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and	Y		
		AU-02.01-04	AU-02 AUDITABLE EVENTS	AU-02.01-04	d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*].	Y		
			AU-02 AUDITABLE EVENTS	Supplemental Guidance	Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system	Y		
		AU-02(1).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(1).01-00	(1) [Withdrawn: Incorporated into AU-12].	Y		
		AU-02(2).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(2).01-00	(2) [Withdrawn: Incorporated into AU-12].	Y		
		AU-02(3).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(3).01-00	(3) The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*].	Y		
			AU-02 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.	Y		
		AU-02(4).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(4).01-00	(4) The organization includes execution of privileged functions in the list of events to be audited by the information system.	Y		
		AU-03.01-00	AU-03 CONTENT OF AUDIT RECORDS	AU-03.01-00	Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	Y		
			AU-03 CONTENT OF AUDIT RECORDS	Supplemental Guidance	Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.	Y		
		AU-03(1).01-00	AU-03 CONTROL ENHANCEMENTS	AU-03(1).01-00	(1) The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject.	Y		
			AU-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.	Y		
		AU-03(2).01-00	AU-03 CONTROL ENHANCEMENTS	AU-03(2).01-00	(2) The organization centrally manages the content of audit records generated by [*Assignment: organization-defined information system components*].	Y		
		AU-04.01-00	AU-04 AUDIT STORAGE CAPACITY	AU-04.01-00	Control: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	Y		
			AU-04 AUDIT STORAGE CAPACITY	Supplemental Guidance	Supplemental Guidance: The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7, SI-4.	Y		
		AU-05.01-00	AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	AU-05.01-00	Control: The information system:	Y		
		AU-05.01-01	AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	AU-05.01-01	a. Alerts designated organizational officials in the event of an audit processing failure; and	Y		
		AU-05.01-02	AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	AU-05.01-02	b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	Y		
			AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	Supplemental Guidance	Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.	Y		
		AU-05(1).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(1).01-00	(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of maximum audit record storage capacity.	Y		
		AU-05(2).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(2).01-00	(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].	Y		
		AU-05(3).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(3).01-00	(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.	Y		
		AU-05(4).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(4).01-00	(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.	Y		
		AU-06.01-00	AU-06 AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-06.01-00	Control: The organization:	Y		
		AU-06.01-00	AU-06 AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-06.01-00	a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and	Y		
		AU-06.01-00	AU-06 AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-06.01-00	b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	Y		
		AU-06(1).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(1).01-00	(1) The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	Y		
		AU-06(2).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(2).01-00	(2) [Withdrawn: Incorporated into SI-4].	Y		
		AU-06(3).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(3).01-00	(3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	Y		
		AU-06(4).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(4).01-00	(4) The information system centralizes the review and analysis of audit records from multiple components within the system.	Y		

		AU-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An example of an automated mechanism for centralized review and analysis is a Security Information Management (SIM) product. Related control: AU-2.	Y		
	AU-06(5).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(5).01-00	(5) The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.	Y		
		AU-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: A Security Event/Information Management system tool can facilitate audit record aggregation and consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by the organization (with localized script	Y		
	AU-06(6).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(6).01-00	(6) The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Y		
		AU-06 CONTROL ENHANCEMENTS			Y		
	AU-06(7).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(7).01-00	(7) The organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.	Y		
		AU-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Permitted actions for information system processes, roles, and/or users associated with the review, analysis, and reporting of audit records include, for example, read, write, append, and delete.	Y		
	AU-06(8).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(8).01-00	(8) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].	Y		
	AU-06(9).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(9).01-00	(9) The organization performs, in a physically dedicated information system, full-text analysis of privileged functions executed.	Y		
	AU-07.01-00	AU-07 AUDIT REDUCTION AND REPORT GENERATION	AU-07.01-00	Control: The information system provides an audit reduction and report generation capability.	Y		
		AU-07 AUDIT REDUCTION AND REPORT GENERATION	Supplemental Guidance	Supplemental Guidance: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. Related control: AU-6.	Y		
	AU-07(1).01-00	AU-07 CONTROL ENHANCEMENTS	AU-07(1).01-00	(1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	Y		
	AU-08.01-00	AU-08 TIME STAMPS	AU-08.01-00	Control: The information system uses internal system clocks to generate time stamps for audit records.	Y		
		AU-08 TIME STAMPS	Supplemental Guidance	Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Related control: AU-3.	Y		
	AU-08(1).01-00	AU-08 CONTROL ENHANCEMENTS	AU-08(1).01-00	(1) The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].	Y		
	AU-09.01-00	AU-09 PROTECTION OF AUDIT INFORMATION	AU-09.01-00	Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Y		
		AU-09 PROTECTION OF AUDIT INFORMATION	Supplemental Guidance	Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.	Y		
	AU-09(1).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(1).01-00	(1) The information system produces audit records on hardware-enforced, write-once media.	Y		
	AU-09(2).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(2).01-00	(2) The information system backs up audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.	Y		
	AU-09(3).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(3).01-00	(3) The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.	Y		
		AU-09 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An example of a cryptographic mechanism for the protection of integrity is the computation and application of a cryptographic-signed hash using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information.	Y		
	AU-09(4).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(4).01-00	(4) The organization:	Y		
	AU-09(4).01-01	AU-09 CONTROL ENHANCEMENTS	AU-09(4).01-01	(a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and	Y		
	AU-09(4).01-02	AU-09 CONTROL ENHANCEMENTS	AU-09(4).01-02	(b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.	Y		
		AU-09 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Auditing may not be reliable when performed by the information system to which the user being audited has privileged access. The privileged user may inhibit auditing or modify audit records. This control enhancement helps mitigate this risk by requiring that privileged access be further defined between audit-	Y		
	AU-10.01-00	AU-10 NON-REPUDIATION	AU-10.01-00	Control: The information system protects against an individual falsely denying having performed a particular action.	Y		
		AU-10 NON-REPUDIATION	Supplemental Guidance	Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not	Y		
	AU-10(1).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(1).01-00	(1) The information system associates the identity of the information producer with the information.	Y		
		AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement supports audit requirements that provide appropriate organizational officials the means to identify who produced specific information in the event of an information transfer. The nature and strength of the binding between the information producer and the information are	Y		
	AU-10(2).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(2).01-00	(2) The information system validates the binding of the information producer's identity to the information.	Y		
		AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is intended to mitigate the risk that information is modified between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums.	Y		
	AU-10(3).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(3).01-00	(3) The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.	Y		
		AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement	Y		
	AU-10(4).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(4).01-00	(4) The information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.	Y		
		AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is intended to mitigate the risk that information is modified between review and transfer/release.	Y		
	AU-10(5).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(5).01-00	(5) The organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.	Y		
	AU-11.01-00	AU-11 AUDIT RECORD RETENTION	AU-11.01-00	Control: The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Y		
		AU-11 AUDIT RECORD RETENTION	Supplemental Guidance	Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard	Y		
	AU-12.01-00	AU-12 AUDIT GENERATION	AU-12.01-00	Control: The information system:	Y		

		AU-12.01-01	AU-12 AUDIT GENERATION	AU-12.01-01	a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*];	Y		
		AU-12.01-02	AU-12 AUDIT GENERATION	AU-12.01-02	b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and	Y		
		AU-12.01-03	AU-12 AUDIT GENERATION	AU-12.01-03	c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	Y		
			AU-12 AUDIT GENERATION	Supplemental Guidance	Supplemental Guidance: Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). Related	Y		
		AU-12(1).01-00	AU-12 CONTROL ENHANCEMENTS	AU-12(1).01-00	(1) The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].	Y		
			AU-12 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.	Y		
		AU-12(2).01-00	AU-12 CONTROL ENHANCEMENTS	AU-12(2).01-00	(2) The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	Y		
			AU-12 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Audit information normalized to a common standard promotes interoperability and exchange of such information between dissimilar devices and information systems. This facilitates an audit system that produces event information that can be more readily analyzed and correlated. System log records and audit	Y		
		AU-13.01-00	AU-13 MONITORING FOR INFORMATION DISCLOSURE	AU-13.01-00	Control: The organization monitors open source information for evidence of unauthorized exfiltration or disclosure of organizational information [*Assignment: organization-defined frequency*].	Y		
		AU-14.01-00	AU-14 SESSION AUDIT	AU-14.01-00	Control: The information system provides the capability to:	Y		
		AU-14.01-01	AU-14 SESSION AUDIT	AU-14.01-01	a. Capture/record and log all content related to a user session; and	Y		
		AU-14.01-02	AU-14 SESSION AUDIT	AU-14.01-02	b. Remotely view/hear all content related to an established user session in real time.	Y		
			AU-14 SESSION AUDIT	Supplemental Guidance	Supplemental Guidance: Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	Y		
		AU-14(1).01-00	AU-14 CONTROL ENHANCEMENTS	AU-14(1).01-00	(1) The information system initiates session audits at system start-up.	Y		
		CA-01.01-00	CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	CA-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		CA-01.01-01	CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	CA-01.01-01	a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		CA-01.01-02	CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	CA-01.01-02	b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	Y		
			CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security assessment and authorization family. The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies,	Y		
		CA-02.01-00	CA-02 SECURITY ASSESSMENTS	CA-02.01-00	Control: The organization:	Y		
		CA-02.01-01	CA-02 SECURITY ASSESSMENTS	CA-02.01-01	a. Develops a security assessment plan that describes the scope of the assessment including:	Y		
		CA-02.01-02	CA-02 SECURITY ASSESSMENTS	CA-02.01-02	b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;	Y		
		CA-02.01-03	CA-02 SECURITY ASSESSMENTS	CA-02.01-03	c. Produces a security assessment report that documents the results of the assessment; and	Y		
		CA-02.01-04	CA-02 SECURITY ASSESSMENTS	CA-02.01-04	d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.	Y		
		CA-02(1).01-00	CA-02 SECURITY ASSESSMENTS	CA-02(1).01-00	(1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	Y		
			CA-02 SECURITY ASSESSMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An independent assessor or assessment team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or	Y		
		CA-02(2).01-00	CA-02 SECURITY ASSESSMENTS	CA-02(2).01-00	(2) The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security testing]*].	Y		
			CA-02 SECURITY ASSESSMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consists of: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine	Y		
		CA-03.01-00	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-00	Control: The organization:	Y		
		CA-03.01-01	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-01	a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;	Y		
		CA-03.01-02	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-02	b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and	Y		
		CA-03.01-03	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-03	c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	Y		
			CA-03 INFORMATION SYSTEM CONNECTIONS	Supplemental Guidance	Supplemental Guidance: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security	Y		
		CA-03(1).01-00	CA-03 CONTROL ENHANCEMENTS	CA-03(1).01-00	(1) The organization prohibits the direct connection of an unclassified, national security system to an external network.	Y		
			CA-03 CONTROL ENHANCEMENTS		Enhancement Supplemental Guidance: An external network is a network that is not controlled by the organization (e.g., the Internet). No direct connection means that an information system cannot connect to an external network without the use of an approved boundary protection device (e.g., firewall) that mediates the communication between	Y		
		CA-03(2).01-00	CA-03 CONTROL ENHANCEMENTS	CA-03(2).01-00	(2) The organization prohibits the direct connection of a classified, national security system to an external network.	Y		
			CA-03 CONTROL ENHANCEMENTS		Enhancement Supplemental Guidance: An external network is a network that is not controlled by the organization (e.g., the Internet). No direct connection means that an information system cannot connect to an external network without the use of an approved boundary protection device (e.g., firewall) that mediates the communication between	Y		
		CA-04.01-00	CA-04 SECURITY CERTIFICATION	CA-04.01-00	[Withdrawn: Incorporated into CA-2].	Y		
		CA-05.01-00	CA-05 PLAN OF ACTION AND MILESTONES	CA-05.01-00	Control: The organization:	Y		
		CA-05.01-01	CA-05 PLAN OF ACTION AND MILESTONES	CA-05.01-01	a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and	Y		

		CA-05.01-02	CA-05 PLAN OF ACTION AND MILESTONES	CA-05.01-02	b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Y		
			CA-05 PLAN OF ACTION AND MILESTONES	Supplemental Guidance	Supplemental Guidance: The plan of action and milestones is a key document in the security authorization package and is subject to federal reporting requirements established by OMB. Related control: PM-4.	Y		
		CA-05(1).01-00	CA-05 CONTROL ENHANCEMENTS	CA-05(1).01-00	(1) The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.	Y		
		CA-06.01-00	CA-06 SECURITY AUTHORIZATION	CA-06.01-00	Control: The organization:	Y		
		CA-06.01-01	CA-06 SECURITY AUTHORIZATION	CA-06.01-01	a. Assigns a senior-level executive or manager to the role of authorizing official for the information system;	Y		
		CA-06.01-02	CA-06 SECURITY AUTHORIZATION	CA-06.01-02	b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and	Y		
		CA-06.01-03	CA-06 SECURITY AUTHORIZATION	CA-06.01-03	c. Updates the security authorization [*Assignment: organization-defined frequency*].	Y		
		CA-07.01-00	CA-07 CONTINUOUS MONITORING	CA-07.01-00	Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:	Y		
		CA-07.01-01	CA-07 CONTINUOUS MONITORING	CA-07.01-01	a. A configuration management process for the information system and its constituent components;	Y		
		CA-07.01-02	CA-07 CONTINUOUS MONITORING	CA-07.01-02	b. A determination of the security impact of changes to the information system and environment of operation;	Y		
		CA-07.01-03	CA-07 CONTINUOUS MONITORING	CA-07.01-03	c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and	Y		
		CA-07.01-04	CA-07 CONTINUOUS MONITORING	CA-07.01-04	d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].	Y		
			CA-07 CONTINUOUS MONITORING	Supplemental Guidance	Supplemental Guidance: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated	Y		
		CA-07(1).01-00	CA-07 CONTROL ENHANCEMENTS	CA-07(1).01-00	(1) The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.	Y		
			CA-07 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental	Y		
		CA-07(2).01-00	CA-07 CONTROL ENHANCEMENTS	CA-07(2).01-00	(2) The organization plans, schedules, and conducts assessments [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security assessment*]] to ensure compliance with all	Y		
			CA-07 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing also provides independent	Y		
		CM-01.01-00	CM-01 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	CM-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		CM-01.01-01	CM-01 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	CM-01.01-01	a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		CM-01.01-02	CM-01 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	CM-01.01-02	b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	Y		
			CM-01 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations,	Y		
		CM-02.01-00	CM-02 BASELINE CONFIGURATION	CM-02.01-00	Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	Y		
			CM-02 BASELINE CONFIGURATION	Supplemental Guidance	Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation,	Y		
		CM-02(1).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-00	(1) The organization reviews and updates the baseline configuration of the information system:	Y		
		CM-02(1).01-01	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-01	(a) [*Assignment: organization-defined frequency*];	Y		
		CM-02(1).01-02	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-02	(b) When required due to [*Assignment organization-defined circumstances*]; and	Y		
		CM-02(1).01-03	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-03	(c) As an integral part of information system component installations and upgrades.	Y		
		CM-02(2).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(2).01-00	(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	Y		
			CM-02 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Software inventory tools are examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems. Software inventory tools can be deployed for each operating system in use within the organization (e.g., on workstations, servers, network components,	Y		
		CM-02(3).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(3).01-00	(3) The organization retains older versions of baseline configurations as deemed necessary to support rollback.	Y		
		CM-02(4).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(4).01-00	(4) The organization:	Y		
		CM-02(4).01-01	CM-02 CONTROL ENHANCEMENTS	CM-02(4).01-01	(a) Develops and maintains [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; and	Y		
		CM-02(4).01-02	CM-02 CONTROL ENHANCEMENTS	CM-02(4).01-02	(b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.	Y		
		CM-02(5).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(5).01-00	(5) The organization:	Y		
		CM-02(5).01-01	CM-02 CONTROL ENHANCEMENTS	CM-02(5).01-01	(a) Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; and	Y		
		CM-02(5).01-02	CM-02 CONTROL ENHANCEMENTS	CM-02(5).01-02	(b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.	Y		
		CM-02(6).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(6).01-00	(6) The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.	Y		
		CM-03.01-00	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-00	Control: The organization:	Y		
		CM-03.01-01	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-01	a. Determines the types of changes to the information system that are configuration controlled;	Y		

		CM-03.01-02	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-02	b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;	Y		
		CM-03.01-03	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-03	c. Documents approved configuration-controlled changes to the system;	Y		
		CM-03.01-04	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-04	d. Retains and reviews records of configuration-controlled changes to the system;	Y		
		CM-03.01-05	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-05	e. Audits activities associated with configuration-controlled changes to the system; and	Y		
		CM-03.01-06	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-06	f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board)*] that convenes [*Selection: (one or more); [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions*]].	Y		
			CM-03 CONFIGURATION CHANGE CONTROL	Supplemental Guidance	Supplemental Guidance: The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and	Y		
		CM-03(1).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-00	(1) The organization employs automated mechanisms to:	Y		
		CM-03(1).01-01	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-01	(a) Document proposed changes to the information system;	Y		
		CM-03(1).01-02	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-02	(b) Notify designated approval authorities;	Y		
		CM-03(1).01-03	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-03	(c) Highlight approvals that have not been received by [*Assignment: organization-defined time period*];	Y		
		CM-03(1).01-04	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-04	(d) Inhibit change until designated approvals are received; and	Y		
		CM-03(1).01-05	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-05	(e) Document completed changes to the information system.	Y		
		CM-03(2).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(2).01-00	(2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	Y		
			CM-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and	Y		
		CM-03(3).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(3).01-00	(3) The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.	Y		
		CM-03(4).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(4).01-00	(4) The organization requires an information security representative to be a member of the [*Assignment: organization-defined configuration change control element (e.g., committee, board)*].	Y		
			CM-03 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Information security representatives can include, for example, Information system security officers or information system security managers. The configuration change control element in this control enhancement is consistent with the change control element defined by the organization in CM-3.	Y		
		CM-04.01-00	CM-04 SECURITY IMPACT ANALYSIS	CM-04.01-00	Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Y		
			CM-04 SECURITY IMPACT ANALYSIS	Supplemental Guidance	Supplemental Guidance: Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact	Y		
		CM-04(1).01-00	CM-04 CONTROL ENHANCEMENTS	CM-04(1).01-00	(1) The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Y		
		CM-04(2).01-00	CM-04 CONTROL ENHANCEMENTS	CM-04(2).01-00	(2) The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.	Y		
		CM-05.01-00	CM-05 ACCESS RESTRICTIONS FOR CHANGE	CM-05.01-00	Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Y		
			CM-05 ACCESS RESTRICTIONS FOR CHANGE	Supplemental Guidance	Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes,	Y		
		CM-05(1).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(1).01-00	(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	Y		
		CM-05(2).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(2).01-00	(2) The organization conducts audits of information system changes [*Assignment: organization-defined frequency*] and when indications so warrant to determine whether unauthorized changes have occurred.	Y		
		CM-05(3).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(3).01-00	(3) The information system prevents the installation of [*Assignment: organization-defined critical software programs*] that are not signed with a certificate that is recognized and approved by the organization.	Y		
			CM-05 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Critical software programs and/or modules include, for example, patches, service packs, and where applicable, device drivers.	Y		
		CM-05(4).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(4).01-00	(4) The organization enforces a two-person rule for changes to [*Assignment: organization-defined information system components and system-level information*].	Y		
		CM-05(5).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(5).01-00	(5) The organization:	Y		
		CM-05(5).01-01	CM-05 CONTROL ENHANCEMENTS	CM-05(5).01-01	(a) Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and	Y		
		CM-05(5).01-02	CM-05 CONTROL ENHANCEMENTS	CM-05(5).01-02	(b) Reviews and reevaluates information system developer/integrator privileges [*Assignment: organization-defined frequency*].	Y		
		CM-05(6).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(6).01-00	(6) The organization limits privileges to change software resident within software libraries (including privileged programs).	Y		
		CM-05(7).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(7).01-00	(7) The information system automatically implements [*Assignment: organization-defined safeguards and countermeasures*] if security functions (or mechanisms) are changed inappropriately.	Y		
			CM-05 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The information system reacts automatically when inappropriate and/or unauthorized modifications have occurred to security functions or mechanisms. Automatic implementation of safeguards and countermeasures includes, for example, reversing the change, halting the information system or triggering an audit	Y		
		CM-06.01-00	CM-06 CONFIGURATION SETTINGS	CM-06.01-00	Control: The organization:	Y		
		CM-06.01-01	CM-06 CONFIGURATION SETTINGS	CM-06.01-01	a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;	Y		
		CM-06.01-02	CM-06 CONFIGURATION SETTINGS	CM-06.01-02	b. Implements the configuration settings;	Y		
		CM-06.01-03	CM-06 CONFIGURATION SETTINGS	CM-06.01-03	c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and	Y		
		CM-06.01-04	CM-06 CONFIGURATION SETTINGS	CM-06.01-04	d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Y		

			CM-06 CONFIGURATION SETTINGS	Supplemental Guidance	Supplemental Guidance: Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-	Y		
		CM-06(1).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(1).01-00	(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.	Y		
		CM-06(2).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(2).01-00	(2) The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].	Y		
			CM-06 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring mandatory/organization-defined configuration settings, or in the extreme case, halting affected information system processing.	Y		
		CM-06(3).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(3).01-00	(3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	Y		
		CM-06(4).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(4).01-00	(4) The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.	Y		
		CM-07.01-00	CM-07 LEAST FUNCTIONALITY	CM-07.01-00	Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*].	Y		
			CM-07 LEAST FUNCTIONALITY	Supplemental Guidance	Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single	Y		
		CM-07(1).01-00	CM-07 CONTROL ENHANCEMENTS	CM-07(1).01-00	(1) The organization reviews the information system [*Assignment: organization-defined frequency*] to identify and eliminate unnecessary functions, ports, protocols, and/or services.	Y		
		CM-07(2).01-00	CM-07 CONTROL ENHANCEMENTS	CM-07(2).01-00	(2) The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].	Y		
		CM-07(3).01-00	CM-07 CONTROL ENHANCEMENTS	CM-07(3).01-00	(3) The organization ensures compliance with [*Assignment: organization-defined registration requirements for ports, protocols, and services*].	Y		
			CM-07 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functionality.	Y		
		CM-08.01-00	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-00	Control: The organization develops, documents, and maintains an inventory of information system components that:	Y		
		CM-08.01-01	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-01	a. Accurately reflects the current information system;	Y		
		CM-08.01-02	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-02	b. Is consistent with the authorization boundary of the information system;	Y		
		CM-08.01-03	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-03	c. Is at the level of granularity deemed necessary for tracking and reporting;	Y		
		CM-08.01-04	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-04	d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and	Y		
		CM-08.01-05	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-05	e. Is available for review and audit by designated organizational officials.	Y		
			CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	Supplemental Guidance	Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked	Y		
		CM-08(1).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(1).01-00	(1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	Y		
		CM-08(2).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(2).01-00	(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	Y		
			CM-08 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Organizations maintain the information system inventory to the extent feasible. Virtual machines, for example, can be difficult to monitor because they are not visible to the network when not in use. In such cases, the intent of this control enhancement is to maintain as up-to-date, complete, and accurate an	Y		
		CM-08(3).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(3).01-00	(3) The organization:	Y		
		CM-08(3).01-01	CM-08 CONTROL ENHANCEMENTS	CM-08(3).01-01	(a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and	Y		
		CM-08(3).01-02	CM-08 CONTROL ENHANCEMENTS	CM-08(3).01-02	(b) Disables network access by such components/devices or notifies designated organizational officials.	Y		
			CM-08 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections in AC-17 and for unauthorized mobile devices in AC-19. The monitoring for unauthorized components/devices on information system networks may be accomplished on an ongoing basis or by the periodic	Y		
		CM-08(4).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(4).01-00	(4) The organization includes in property accountability information for information system components, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components.	Y		
		CM-08(5).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(5).01-00	(5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	Y		
		CM-08(6).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(6).01-00	(6) The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.	Y		
			CM-08 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement focuses on the configuration settings established by the organization for its information system components, the specific information system components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established	Y		
		CM-09.01-00	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-00	Control: The organization develops, documents, and implements a configuration management plan for the information system that:	Y		
		CM-09.01-01	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-01	a. Addresses roles, responsibilities, and configuration management processes and procedures;	Y		
		CM-09.01-02	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-02	b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and	Y		
		CM-09.01-03	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-03	c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	Y		
			CM-09 CONFIGURATION MANAGEMENT PLAN	Supplemental Guidance	Supplemental Guidance: Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The	Y		
		CM-09(1).01-00	CM-09 CONTROL ENHANCEMENTS	CM-09(1).01-00	(1) The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.	Y		
			CM-09 CONTROL ENHANCEMENTS	Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process.	Y		
		CP-01.01-00	CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES	CP-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		CP-01.01-01		CP-01.01-01	a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		

		CP-01.01-02		CP-01.01-02	b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	Y			
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations,	Y			
		CP-02.01-00	CP-2 CONTINGENCY PLAN	CP-02.01-00	Control: The organization:	Y			
		CP-02.01-01		CP-02.01-01	a. Develops a contingency plan for the information system that:	Y			
		CP-02.01-02		CP-02.01-02	b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*];	Y			
		CP-02.01-03		CP-02.01-03	c. Coordinates contingency planning activities with incident handling activities;	Y			
		CP-02.01-04		CP-02.01-04	d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];	Y			
		CP-02.01-05		CP-02.01-05	e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and	Y			
		CP-02.01-06		CP-02.01-06	f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].	Y			
				Supplemental Guidance	Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised.	Y			
		CP-02(1).01-00	Control Enhancements:	CP-02(1).01-00	(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.	Y			
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.	Y			
		CP-02(2).01-00	Control Enhancements:	CP-02(2).01-00	(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	Y			
		CP-02(3).01-00	Control Enhancements:	CP-02(3).01-00	(3) The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.	Y			
		CP-02(4).01-00	Control Enhancements:	CP-02(4).01-00	(4) The organization plans for the full resumption of missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.	Y			
		CP-02(5).01-00	Control Enhancements:	CP-02(5).01-00	(5) The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	Y			
		CP-02(6).01-00	Control Enhancements:	CP-02(6).01-00	(6) The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.	Y			
		CP-03.01-00	CP-3 CONTINGENCY TRAINING	CP-03.01-00	Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].	Y			
		CP-03(1).01-00	Control Enhancements:	CP-03(1).01-00	(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Y			
		CP-03(2).01-00	Control Enhancements:	CP-03(2).01-00	(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	Y			
		CP-04.01-00	CP-4 CONTINGENCY PLAN TESTING AND EXERCISES	CP-04.01-00	Control: The organization:	Y			
		CP-04.01-01		CP-04.01-01	a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and	Y			
		CP-04.01-02		CP-04.01-02	b. Reviews the contingency plan test/exercise results and initiates corrective actions.	Y			
				Supplemental Guidance	Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in	Y			
		CP-04(1).01-00	Control Enhancements:	CP-04(1).01-00	(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	Y			
					Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.	Y			
		CP-04(2).01-00	Control Enhancements:	CP-04(2).01-00	(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.	Y			
		CP-04(3).01-00	Control Enhancements:	CP-04(3).01-00	(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.	Y			
		CP-04(4).01-00	Control Enhancements:	CP-04(4).01-00	(4) The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.	Y			
		CP-05.01-00	CP-5 CONTINGENCY PLAN UPDATE	CP-05.01-00	[Withdrawn: Incorporated into CP-2].	Y			
		CP-06.01-00	CP-6 ALTERNATE STORAGE SITE	CP-06.01-00	Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.	Y			
		CP-06(1).01-00	Control Enhancements:	CP-06(1).01-00	(1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	Y			
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.	Y			
		CP-06(2).01-00	Control Enhancements:	CP-06(2).01-00	(2) The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Y			
		CP-06(3).01-00	Control Enhancements:	CP-06(3).01-00	(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Y			
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.	Y			
		CP-07.01-00	CP-7 ALTERNATE PROCESSING SITE	CP-07.01-00	Control: The organization:	Y			
		CP-07.01-01		CP-07.01-01	a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; and	Y			
		CP-07.01-02		CP-07.01-02	b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.	Y			

		CP-07(1).01-00	Control Enhancements:	CP-07(1).01-00	(1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	Y		
					Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.	Y		
		CP-07(2).01-00	Control Enhancements:	CP-07(2).01-00	(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Y		
		CP-07(3).01-00	Control Enhancements:	CP-07(3).01-00	(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	Y		
		CP-07(4).01-00	Control Enhancements:	CP-07(4).01-00	(4) The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.	Y		
		CP-07(5).01-00	Control Enhancements:	CP-07(5).01-00	(5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	Y		
		CP-08.01-00	CP-8 TELECOMMUNICATIONS SERVICES	CP-08.01-00	Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.	Y		
		CP-08(1).01-00	Control Enhancements:	CP-08(1).01-00	(1) The organization:	Y		
		CP-08(1).01-01	Control Enhancements:	CP-08(1).01-01	(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and	Y		
		CP-08(1).01-02	Control Enhancements:	CP-08(1).01-02	(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	Y		
		CP-08(2).01-00	Control Enhancements:	CP-08(2).01-00	(2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	Y		
		CP-08(3).01-00	Control Enhancements:	CP-08(3).01-00	(3) The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.	Y		
		CP-08(4).01-00	Control Enhancements:	CP-08(4).01-00	(4) The organization requires primary and alternate telecommunications service providers to have contingency plans.	Y		
		CP-09.01-00	CP-9 INFORMATION SYSTEM BACKUP	CP-09.01-00	Control: The organization:	Y		
		CP-09.01-01		CP-09.01-01	a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];	Y		
		CP-09.01-02		CP-09.01-02	b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];	Y		
		CP-09.01-03		CP-09.01-03	c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and	Y		
		CP-09.01-04		CP-09.01-04	d. Protects the confidentiality and integrity of backup information at the storage location.	Y		
				Supplemental Guidance	Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of	Y		
		CP-09(1).01-00	Control Enhancements:	CP-09(1).01-00	(1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.	Y		
		CP-09(2).01-00	Control Enhancements:	CP-09(2).01-00	(2) The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	Y		
		CP-09(3).01-00	Control Enhancements:	CP-09(3).01-00	(3) The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.	Y		
		CP-09(4).01-00	Control Enhancements:	CP-09(4).01-00	(4) [Withdrawn: Incorporated into CP-9].	Y		
		CP-09(5).01-00	Control Enhancements:	CP-09(5).01-00	(5) The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].	Y		
		CP-09(6).01-00	Control Enhancements:	CP-09(6).01-00	(6) The organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.	Y		
		CP-10.01-00	CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	CP-10.01-00	Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	Y		
				Supplemental Guidance	Supplemental Guidance: Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution	Y		
		CP-10(1).01-00	Control Enhancements:	CP-10(1).01-00	(1) [Withdrawn: Incorporated into CP-4].	Y		
		CP-10(2).01-00	Control Enhancements:	CP-10(2).01-00	(2) The information system implements transaction recovery for systems that are transaction-based.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.	Y		
		CP-10(3).01-00	Control Enhancements:	CP-10(3).01-00	(3) The organization provides compensating security controls for [*Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state*].	Y		
		CP-10(4).01-00	Control Enhancements:	CP-10(4).01-00	(4) The organization provides the capability to reimage information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.	Y		
		CP-10(5).01-00	Control Enhancements:	CP-10(5).01-00	(5) The organization provides [*Selection: real-time; near-real-time*] [*Assignment: organization-defined failover capability for the information system*].	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Examples of failover capability are incorporating mirrored information system operations at an alternate processing site or periodic data mirroring at regular intervals during a time period defined by the organization's recovery time period.	Y		
		CP-10(6).01-00	Control Enhancements:	CP-10(6).01-00	(6) The organization protects backup and restoration hardware, firmware, and software.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software includes both physical and technical measures. Router tables, compilers, and other security-relevant system software are examples of backup and restoration software.	Y		
		IA-01.01-00	IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	IA-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		IA-01.01-01		IA-01.01-01	a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		IA-01.01-02		IA-01.01-02	b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	Y		

					Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies,	Y		
			IA-02.01-00	IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-02.01-00	Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Y		
					Supplemental Guidance	Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented	Y		
			IA-02(1).01-00	Control Enhancements:	IA-02(1).01-00	(1) The information system uses multifactor authentication for network access to privileged accounts.	Y		
			IA-02(2).01-00	Control Enhancements:	IA-02(2).01-00	(2) The information system uses multifactor authentication for network access to non-privileged accounts.	Y		
			IA-02(3).01-00	Control Enhancements:	IA-02(3).01-00	(3) The information system uses multifactor authentication for local access to privileged accounts.	Y		
			IA-02(4).01-00	Control Enhancements:	IA-02(4).01-00	(4) The information system uses multifactor authentication for local access to non-privileged accounts.	Y		
			IA-02(5).01-00	Control Enhancements:	IA-02(5).01-00	(5) The organization:	Y		
			IA-02(5).01-01	Control Enhancements:	IA-02(5).01-01	(a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and	Y		
			IA-02(5).01-02	Control Enhancements:	IA-02(5).01-02	(b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.	Y		
			IA-02(6).01-00	Control Enhancements:	IA-02(6).01-00	(6) The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.	Y		
			IA-02(7).01-00	Control Enhancements:	IA-02(7).01-00	(7) The information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.	Y		
			IA-02(8).01-00	Control Enhancements:	IA-02(8).01-00	(8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-	Y		
			IA-02(9).01-00	Control Enhancements:	IA-02(9).01-00	(9) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to non-privileged accounts.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-	Y		
			IA-03.01-00	IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION	IA-03.01-00	Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.	Y		
					Supplemental Guidance	Supplemental Guidance: The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control	Y		
			IA-03(1).01-00	Control Enhancements:	IA-03(1).01-00	(1) The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Remote network connection is any connection with a device communicating through an external network (e.g., the Internet). Related controls: AC-17, AC-18.	Y		
			IA-03(2).01-00	Control Enhancements:	IA-03(2).01-00	(2) The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.	Y		
			IA-03(3).01-00	Control Enhancements:	IA-03(3).01-00	(3) The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: With regard to dynamic address allocation for devices, DHCP-enabled clients typically obtain *leases* for IP addresses from DHCP servers.	Y		
			IA-04.01-00	IA-4 IDENTIFIER MANAGEMENT	IA-04.01-00	Control: The organization manages information system identifiers for users and devices by:	Y		
			IA-04.01-01		IA-04.01-01	a. Receiving authorization from a designated organizational official to assign a user or device identifier;	Y		
			IA-04.01-02		IA-04.01-02	b. Selecting an identifier that uniquely identifies an individual or device;	Y		
			IA-04.01-03		IA-04.01-03	c. Assigning the user identifier to the intended party or the device identifier to the intended device;	Y		
			IA-04.01-04		IA-04.01-04	d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and	Y		
			IA-04.01-05		IA-04.01-05	e. Disabling the user identifier after [Assignment: organization-defined time period of inactivity].	Y		
					Supplemental Guidance	Supplemental Guidance: Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an	Y		
							Y		
			IA-04(1).01-00	Control Enhancements:	IA-04(1).01-00	(1) The organization prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address).	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The organization implements this control enhancement to the extent that the information system allows.	Y		
			IA-04(2).01-00	Control Enhancements:	IA-04(2).01-00	(2) The organization requires that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority.	Y		
			IA-04(3).01-00	Control Enhancements:	IA-04(3).01-00	(3) The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.	Y		
			IA-04(4).01-00	Control Enhancements:	IA-04(4).01-00	(4) The organization manages user identifiers by uniquely identifying the user as [*Assignment: organization-defined characteristic identifying user status*].	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Characteristics identifying user status include, for example, contractors and foreign nationals.	Y		
			IA-04(5).01-00	Control Enhancements:	IA-04(5).01-00	(5) The information system dynamically manages identifiers, attributes, and associated access authorizations.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: In contrast to conventional approaches to identification and authentication which employ static information system accounts for preregistered users, many service-oriented architecture implementations rely on establishing identities at run time for entities that were previously unknown. Dynamic	Y		

	IA-05.01-00	IA-5 AUTHENTICATOR MANAGEMENT	IA-05.01-00	Control: The organization manages information system authenticators for users and devices by:	Y		
	IA-05.01-01		IA-05.01-01	a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;	Y		
	IA-05.01-02		IA-05.01-02	b. Establishing initial authenticator content for authenticators defined by the organization;	Y		
	IA-05.01-03		IA-05.01-03	c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;	Y		
	IA-05.01-04		IA-05.01-04	d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;	Y		
	IA-05.01-05		IA-05.01-05	e. Changing default content of authenticators upon information system installation;	Y		
	IA-05.01-06		IA-05.01-06	f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);	Y		
	IA-05.01-07		IA-05.01-07	g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];	Y		
	IA-05.01-08		IA-05.01-08	h. Protecting authenticator content from unauthorized disclosure and modification; and	Y		
	IA-05.01-09		IA-05.01-09	i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.	Y		
			Supplemental Guidance	Supplemental Guidance: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with	Y		
	IA-05(1).01-00	Control Enhancements:	IA-05(1).01-00	(1) The information system, for password-based authentication:	Y		
	IA-05(1).01-01	Control Enhancements:	IA-05(1).01-01	(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];	Y		
	IA-05(1).01-02	Control Enhancements:	IA-05(1).01-02	(b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created;	Y		
	IA-05(1).01-03	Control Enhancements:	IA-05(1).01-03	(c) Encrypts passwords in storage and in transmission;	Y		
	IA-05(1).01-04	Control Enhancements:	IA-05(1).01-04	(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and	Y		
	IA-05(1).01-05	Control Enhancements:	IA-05(1).01-05	(e) Prohibits password reuse for [Assignment: organization-defined number] generations.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does *not* apply to situations where passwords are used to unlock hardware	Y		
	IA-05(2).01-00	Control Enhancements:	IA-05(2).01-00	(2) The information system, for PKI-based authentication:	Y		
	IA-05(2).01-01	Control Enhancements:	IA-05(2).01-01	(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor;	Y		
	IA-05(2).01-02	Control Enhancements:	IA-05(2).01-02	(b) Enforces authorized access to the corresponding private key; and	Y		
	IA-05(2).01-03	Control Enhancements:	IA-05(2).01-03	(c) Maps the authenticated identity to the user account.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.	Y		
	IA-05(3).01-00	Control Enhancements:	IA-05(3).01-00	(3) The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	Y		
	IA-05(4).01-00	Control Enhancements:	IA-05(4).01-00	(4) The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.	Y		
	IA-05(5).01-00	Control Enhancements:	IA-05(5).01-00	(5) The organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators for those	Y		
	IA-05(6).01-00	Control Enhancements:	IA-05(6).01-00	(6) The organization protects authenticators commensurate with the classification or sensitivity of the information accessed.	Y		
	IA-05(7).01-00	Control Enhancements:	IA-05(7).01-00	(7) The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Organizations exercise caution in determining whether an embedded or stored authenticator is in encrypted or unencrypted form. If the authenticator in its stored representation, is used in the manner stored, then that representation is considered an unencrypted authenticator. This is irrespective of whether that	Y		
	IA-05(8).01-00	Control Enhancements:	IA-05(8).01-00	(8) The organization takes [*Assignment: organization-defined measures*] to manage the risk of compromise due to individuals having accounts on multiple information systems.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: When an individual has accounts on multiple information systems, there is the risk that if one account is compromised and the individual is using the same user identifier and authenticator, other accounts will be compromised as well. Possible alternatives include, but are not limited to: (1) having the same user	Y		
	IA-06.01-00	IA-6 AUTHENTICATOR FEEDBACK	IA-06.01-00	Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Y		
			Supplemental Guidance	Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.	Y		
	IA-07.01-00	IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-07.01-00	Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	Y		
	IA-08.01-00	IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-08.01-00	Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Y		
			Supplemental Guidance	Supplemental Guidance: Non-organizational users include all information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. In accordance with the E-	Y		
	IR-01.01-00	IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES	IR-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
	IR-01.01-01		IR-01.01-01	a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		

		IR-01.01-02		IR-01.01-02	b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards,	Y		
		IR-02.01-00	IR-2 INCIDENT RESPONSE TRAINING	IR-02.01-00	Control: The organization:	Y		
		IR-02.01-01		IR-02.01-01	a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and	Y		
		IR-02.01-02		IR-02.01-02	b. Provides refresher training [*Assignment: organization-defined frequency*].	Y		
					Supplemental Guidance: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.	Y		
		IR-02(1).01-00	Control Enhancements:	IR-02(1).01-00	(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.	Y		
		IR-02(2).01-00	Control Enhancements:	IR-02(2).01-00	(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	Y		
		IR-03.01-00	IR-3 INCIDENT RESPONSE TESTING AND EXERCISES	IR-03.01-00	Control: The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.	Y		
		IR-03(1).01-00	Control Enhancements:	IR-03(1).01-00	(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response	Y		
		IR-04.01-00	IR-4 INCIDENT HANDLING	IR-04.01-00	Control: The organization:	Y		
		IR-04.01-01		IR-04.01-01	a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;	Y		
		IR-04.01-02		IR-04.01-02	b. Coordinates incident handling activities with contingency planning activities; and	Y		
		IR-04.01-03		IR-04.01-03	c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	Y		
				Supplemental Guidance	Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	Y		
		IR-04(1).01-00	Control Enhancements:	IR-04(1).01-00	(1) The organization employs automated mechanisms to support the incident handling process.	Y		
					Enhancement Supplemental Guidance: An online incident management system is an example of an automated mechanism.	Y		
		IR-04(2).01-00	Control Enhancements:	IR-04(2).01-00	(2) The organization includes dynamic reconfiguration of the information system as part of the incident response capability.	Y		
					Enhancement Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways.	Y		
		IR-04(3).01-00	Control Enhancements:	IR-04(3).01-00	(3) The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions that may be appropriate include, for example, graceful degradation, information system shutdown, fall back to manual	Y		
		IR-04(4).01-00	Control Enhancements:	IR-04(4).01-00	(4) The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Y		
		IR-04(5).01-00	Control Enhancements:	IR-04(5).01-00	(5) The organization implements a configurable capability to automatically disable the information system if any of the following security violations are detected: [*Assignment: organization-defined list of security violations*].	Y		
		IR-05.01-00	IR-5 INCIDENT MONITORING	IR-05.01-00	Control: The organization tracks and documents information system security incidents.	Y		
				Supplemental Guidance	Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for	Y		
						Y		
		IR-05(1).01-00	Control Enhancements:	IR-05(1).01-00	(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-6, AU-7, SI-4.	Y		
		IR-06.01-00	IR-6 INCIDENT REPORTING	IR-06.01-00	Control: The organization:	Y		
		IR-06.01-01		IR-06.01-01	a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and	Y		
		IR-06.01-02		IR-06.01-02	b. Reports security incident information to designated authorities.	Y		
				Supplemental Guidance	Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of	Y		
		IR-06(1).01-00	Control Enhancements:	IR-06(1).01-00	(1) The organization employs automated mechanisms to assist in the reporting of security incidents.	Y		
		IR-06(2).01-00	Control Enhancements:	IR-06(2).01-00	(2) The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.	Y		
		IR-07.01-00	IR-7 INCIDENT RESPONSE ASSISTANCE	IR-07.01-00	Control: The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Y		
				Supplemental Guidance	Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.	Y		
						Y		
		IR-07(1).01-00	Control Enhancements:	IR-07(1).01-00	(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	Y		

				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general	Y		
		IR-07(2).01-00	Control Enhancements:	IR-07(2).01-00	(2) The organization:	Y		
		IR-07(2).01-01	Control Enhancements:	IR-07(2).01-01	(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and	Y		
		IR-07(2).01-02	Control Enhancements:	IR-07(2).01-02	(b) Identifies organizational incident response team members to the external providers.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and	Y		
		IR-08.01-00	IR-8 INCIDENT RESPONSE PLAN	IR-08.01-00	Control: The organization:	Y		
		IR-08.01-01		IR-08.01-01	a. Develops an incident response plan that:	Y		
		IR-08.01-02		IR-08.01-02	b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*];	Y		
		IR-08.01-03		IR-08.01-03	c. Reviews the incident response plan [*Assignment: organization-defined frequency*];	Y		
		IR-08.01-04		IR-08.01-04	d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and	Y		
		IR-08.01-05		IR-08.01-05	e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	Y		
				Supplemental Guidance	Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.	Y		
		MA-01.01-00	MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES	MA-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		MA-01.01-01		MA-01.01-01	a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		MA-01.01-02		MA-01.01-02	b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations,	Y		
		MA-02.01-00	MA-2 CONTROLLED MAINTENANCE	MA-02.01-00	Control: The organization:	Y		
		MA-02.01-01		MA-02.01-01	a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;	Y		
		MA-02.01-02		MA-02.01-02	b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;	Y		
		MA-02.01-03		MA-02.01-03	c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;	Y		
		MA-02.01-04		MA-02.01-04	d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and	Y		
		MA-02.01-05		MA-02.01-05	e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	Y		
				Supplemental Guidance	Supplemental Guidance: The control is intended to address the information security aspects of the organization's information system maintenance program. Related controls: MP-6, SI-2.	Y		
		MA-02(1).01-00	Control Enhancements:	MA-02(1).01-00	(1) The organization maintains maintenance records for the information system that include:	Y		
		MA-02(1).01-01	Control Enhancements:	MA-02(1).01-01	(a) Date and time of maintenance;	Y		
		MA-02(1).01-02	Control Enhancements:	MA-02(1).01-02	(b) Name of the individual performing the maintenance;	Y		
		MA-02(1).01-03	Control Enhancements:	MA-02(1).01-03	(c) Name of escort, if necessary;	Y		
		MA-02(1).01-04	Control Enhancements:	MA-02(1).01-04	(d) A description of the maintenance performed; and	Y		
		MA-02(1).01-05	Control Enhancements:	MA-02(1).01-05	(e) A list of equipment removed or replaced (including identification numbers, if applicable).	Y		
		MA-02(2).01-00	Control Enhancements:	MA-02(2).01-00	(2) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.	Y		
		MA-03.01-00	MA-3 MAINTENANCE TOOLS	MA-03.01-00	Control: The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	Y		
				Supplemental Guidance	Supplemental Guidance: The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software	Y		
		MA-03(1).01-00	Control Enhancements:	MA-03(1).01-00	(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.	Y		
		MA-03(2).01-00	Control Enhancements:	MA-03(2).01-00	(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	Y		
		MA-03(3).01-00	Control Enhancements:	MA-03(3).01-00	(3) The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official	Y		
		MA-03(4).01-00	Control Enhancements:	MA-03(4).01-00	(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.	Y		
		MA-04.01-00	MA-4 NON-LOCAL MAINTENANCE	MA-04.01-00	Control: The organization:	Y		
		MA-04.01-01		MA-04.01-01	a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities;	Y		

		MA-04.01-02		MA-04.01-02	b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;	Y		
		MA-04.01-03		MA-04.01-03	c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;	Y		
		MA-04.01-04		MA-04.01-04	d. Maintains records for non-local maintenance and diagnostic activities; and	Y		
		MA-04.01-05		MA-04.01-05	e. Terminates all sessions and network connections when non-local maintenance is completed.	Y		
				Supplemental Guidance	Supplemental Guidance: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information	Y		
		MA-04(1).01-00	Control Enhancements:	MA-04(1).01-00	(1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.	Y		
		MA-04(2).01-00	Control Enhancements:	MA-04(2).01-00	(2) The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	Y		
		MA-04(3).01-00	Control Enhancements:	MA-04(3).01-00	(3) The organization:	Y		
		MA-04(3).01-01	Control Enhancements:	MA-04(3).01-01	(a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or	Y		
		MA-04(3).01-02	Control Enhancements:	MA-04(3).01-02	(b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially	Y		
		MA-04(4).01-00	Control Enhancements:	MA-04(4).01-00	(4) The organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either:	Y		
		MA-04(4).01-01	Control Enhancements:	MA-04(4).01-01	(a) Physically separated communications paths; or	Y		
		MA-04(4).01-02	Control Enhancements:	MA-04(4).01-02	(b) Logically separated communications paths based upon encryption.	Y		
		MA-04(5).01-00	Control Enhancements:	MA-04(5).01-00	(5) The organization requires that:	Y		
		MA-04(5).01-01	Control Enhancements:	MA-04(5).01-01	(a) Maintenance personnel notify [*Assignment: organization-defined personnel*] when non-local maintenance is planned (i.e., date/time); and	Y		
		MA-04(5).01-02	Control Enhancements:	MA-04(5).01-02	(b) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance.	Y		
		MA-04(6).01-00	Control Enhancements:	MA-04(6).01-00	(6) The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.	Y		
		MA-04(7).01-00	Control Enhancements:	MA-04(7).01-00	(7) The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.	Y		
		MA-05.01-00	MA-5 MAINTENANCE PERSONNEL	MA-05.01-00	Control: The organization:	Y		
		MA-05.01-01		MA-05.01-01	a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and	Y		
		MA-05.01-02		MA-05.01-02	b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access	Y		
				Supplemental Guidance	Supplemental Guidance: Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue	Y		
		MA-05(1).01-00	Control Enhancements:	MA-05(1).01-00	(1) The organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:	Y		
		MA-05(1).01-01	Control Enhancements:	MA-05(1).01-01	(a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are	Y		
		MA-05(1).01-02	Control Enhancements:	MA-05(1).01-02	(b) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and	Y		
		MA-05(1).01-03	Control Enhancements:	MA-05(1).01-03	(c) In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The intent of this control enhancement is to deny individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled	Y		
		MA-05(2).01-00	Control Enhancements:	MA-05(2).01-00	(2) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are cleared (i.e., possess appropriate security clearances) for the highest level of information on the system.	Y		
		MA-05(3).01-00	Control Enhancements:	MA-05(3).01-00	(3) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.	Y		
		MA-05(4).01-00	Control Enhancements:	MA-05(4).01-00	(4) The organization ensures that:	Y		
		MA-05(4).01-01	Control Enhancements:	MA-05(4).01-01	(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on an information system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and	Y		
		MA-05(4).01-02	Control Enhancements:	MA-05(4).01-02	(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on an information system are fully documented within a Memorandum of Agreement.	Y		
		MA-06.01-00	MA-6 TIMELY MAINTENANCE	MA-06.01-00	Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.	Y		
				Supplemental Guidance	Supplemental Guidance: The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways,	Y		
		MP-01.01-00	MP-1 MEDIA PROTECTION POLICY AND PROCEDURES	MP-01.01-00	Control: The organization: develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		MP-01.01-01		MP-01.01-01	a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		MP-01.01-02		MP-01.01-02	b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards,	Y		
		MP-02.01-00	MP-2 MEDIA ACCESS	MP-02.01-00	Control: The organization restricts access to [*Assignment: organization-defined types of digital and non-digital media*] to [*Assignment: organization-defined list of authorized individuals*] using [*Assignment: organization-defined security measures*].	Y		

				Supplemental Guidance	Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability	Y		
		MP-02(1).01-00	Control Enhancements:	MP-02(1).01-00	(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices).	Y		
		MP-02(2).01-00		MP-02(2).01-00	(2) The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.	Y		
		MP-03.01-00	MP-3 MEDIA MARKING	MP-03.01-00	Control: The organization:	Y		
		MP-03.01-01		MP-03.01-01	a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and	Y		
		MP-03.01-02		MP-03.01-02	b. Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].	Y		
				Supplemental Guidance	Supplemental Guidance: The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system	Y		
		MP-04.01-00	MP-4 MEDIA STORAGE	MP-04.01-00	Control: The organization:	Y		
		MP-04.01-01		MP-04.01-01	a. Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*];	Y		
		MP-04.01-02		MP-04.01-02	b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Y		
		MP-04(1).01-00	Control Enhancements:	MP-04(1).01-00	(1) The organization employs cryptographic mechanisms to protect information in storage.	Y		
		MP-05.01-00	MP-5 MEDIA TRANSPORT	MP-05.01-00	Control: The organization:	Y		
		MP-05.01-01		MP-05.01-01	a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined security measures*];	Y		
		MP-05.01-02		MP-05.01-02	b. Maintains accountability for information system media during transport outside of controlled areas; and	Y		
		MP-05.01-03		MP-05.01-03	c. Restricts the activities associated with transport of such media to authorized personnel.	Y		
						Y		
		MP-05(1).01-00	Control Enhancements:	MP-05(1).01-00	(1) [Withdrawn: Incorporated into MP-5].	Y		
		MP-05(2).01-00	Control Enhancements:	MP-05(2).01-00	(2) The organization documents activities associated with the transport of information system media.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of	Y		
		MP-05(3).01-00	Control Enhancements:	MP-05(3).01-00	(3) The organization employs an identified custodian throughout the transport of information system media.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.	Y		
		MP-05(4).01-00	Control Enhancements:	MP-05(4).01-00	(4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones).	Y		
		MP-06.01-00	MP-6 MEDIA SANITIZATION	MP-06.01-00	Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.	Y		
				Supplemental Guidance	Supplemental Guidance: This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing,	Y		
		MP-06(1).01-00	Control Enhancements:	MP-06(1).01-00	(1) The organization tracks, documents, and verifies media sanitization and disposal actions.	Y		
		MP-06(2).01-00	Control Enhancements:	MP-06(2).01-00	(2) The organization tests sanitization equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].	Y		
		MP-06(3).01-00	Control Enhancements:	MP-06(3).01-00	(3) The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices*].	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily	Y		
		MP-06(4).01-00	Control Enhancements:	MP-06(4).01-00	(4) The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.	Y		
		MP-06(5).01-00	Control Enhancements:	MP-06(5).01-00	(5) The organization sanitizes information system media containing classified information in accordance with NSA standards and policies.	Y		
		MP-06(6).01-00	Control Enhancements:	MP-06(6).01-00	(6) The organization destroys information system media that cannot be sanitized.	Y		
		PE-01.01-00	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	PE-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		PE-01.01-01		PE-01.01-01	a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		PE-01.01-02		PE-01.01-02	b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies,	Y		
		PE-02.01-00	PE-2 PHYSICAL ACCESS AUTHORIZATIONS	PE-02.01-00	Control: The organization:	Y		
		PE-02.01-01		PE-02.01-01	a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);	Y		

			PE-02.01-02		PE-02.01-02	b. Issues authorization credentials;	Y		
			PE-02.01-03		PE-02.01-03	c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.	Y		
					Supplemental Guidance	Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. Related control: PE-3, PE-4.	Y		
			PE-02(1).01-00	Control Enhancements:	PE-02(1).01-00	(1) The organization authorizes physical access to the facility where the information system resides based on position or role.	Y		
			PE-02(2).01-00	Control Enhancements:	PE-02(2).01-00	(2) The organization requires two forms of identification to gain access to the facility where the information system resides.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Examples of forms of identification are identification badge, key card, cipher PIN, and biometrics.	Y		
			PE-02(3).01-00	Control Enhancements:	PE-02(3).01-00	(3) The organization restricts physical access to the facility containing an information system that processes classified information to authorized personnel with appropriate clearances and access authorizations.	Y		
			PE-03.01-00	PE-3 PHYSICAL ACCESS CONTROL	PE-03.01-00	Control: The organization:	Y		
			PE-03.01-01		PE-03.01-01	a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);	Y		
			PE-03.01-02		PE-03.01-02	b. Verifies individual access authorizations before granting access to the facility;	Y		
			PE-03.01-03		PE-03.01-03	c. Controls entry to the facility containing the information system using physical access devices and/or guards;	Y		
			PE-03.01-04		PE-03.01-04	d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;	Y		
			PE-03.01-05		PE-03.01-05	e. Secures keys, combinations, and other physical access devices;	Y		
			PE-03.01-06		PE-03.01-06	f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and	Y		
			PE-03.01-07		PE-03.01-07	g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Y		
					Supplemental Guidance	Supplemental Guidance: The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated	Y		
			PE-03(1).01-00	Control Enhancements:	PE-03(1).01-00	(1) The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the	Y		
			PE-03(2).01-00	Control Enhancements:	PE-03(2).01-00	(2) The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.	Y		
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The extent/frequency or randomness of the checks is as deemed necessary by the organization to adequately mitigate risk associated with exfiltration.	Y		
			PE-03(3).01-00	Control Enhancements:	PE-03(3).01-00	(3) The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.	Y		
			PE-03(4).01-00	Control Enhancements:	PE-03(4).01-00	(4) The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.	Y		
			PE-03(5).01-00	Control Enhancements:	PE-03(5).01-00	(5) The information system detects/prevents physical tampering or alteration of hardware components within the system.	Y		
			PE-03(6).01-00	Control Enhancements:	PE-03(6).01-00	(6) The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.	Y		
			PE-04.01-00	PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM	PE-04.01-00	Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.	Y		
					Supplemental Guidance	Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control	Y		
			PE-05.01-00	PE-5 ACCESS CONTROL FOR OUTPUT DEVICES	PE-05.01-00	Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Y		
					Supplemental Guidance	Supplemental Guidance: Monitors, printers, and audio devices are examples of information system output devices.	Y		
			PE-06.01-00	PE-6 MONITORING PHYSICAL ACCESS	PE-06.01-00	Control: The organization:	Y		
			PE-06.01-01		PE-06.01-01	a. Monitors physical access to the information system to detect and respond to physical security incidents;	Y		
			PE-06.01-02		PE-06.01-02	b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and	Y		
			PE-06.01-03		PE-06.01-03	c. Coordinates results of reviews and investigations with the organization's incident response capability.	Y		
					Supplemental Guidance	Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.	Y		
							Y		
			PE-06(1).01-00	Control Enhancements:	PE-06(1).01-00	(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.	Y		
			PE-06(2).01-00	Control Enhancements:	PE-06(2).01-00	(2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.	Y		
			PE-07.01-00	PE-7 VISITOR CONTROL	PE-07.01-00	Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	Y		
					Supplemental Guidance	Supplemental Guidance: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.	Y		
			PE-07(1).01-00	Control Enhancements:	PE-07(1).01-00	(1) The organization escorts visitors and monitors visitor activity, when required.	Y		

PE-07(2).01-00	Control Enhancements:	PE-07(2).01-00	(2) The organization requires two forms of identification for visitor access to the facility.	Y			
PE-08.01-00	PE-8 ACCESS RECORDS	PE-08.01-00	Control: The organization:	Y			
PE-08.01-01		PE-08.01-01	a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and	Y			
PE-08.01-02		PE-08.01-02	b. Reviews visitor access records [*Assignment: organization-defined frequency*].	Y			
		Supplemental Guidance	Supplemental Guidance: Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.	Y			
PE-08(1).01-00	Control Enhancements:	PE-08(1).01-00	(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.	Y			
PE-08(2).01-00	Control Enhancements:	PE-08(2).01-00	(2) The organization maintains a record of all physical access, both visitor and authorized individuals.	Y			
PE-09.01-00	PE-9 POWER EQUIPMENT AND POWER CABLING	PE-09.01-00	Control: The organization protects power equipment and power cabling for the information system from damage and destruction.	Y			
		Supplemental Guidance	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	Y			
PE-09(1).01-00	Control Enhancements:	PE-09(1).01-00	(1) The organization employs redundant and parallel power cabling paths.	Y			
PE-09(2).01-00	Control Enhancements:	PE-09(2).01-00	(2) The organization employs automatic voltage controls for [*Assignment: organization-defined list of critical information system components*].	Y			
PE-10.01-00	PE-10 EMERGENCY SHUTOFF	PE-10.01-00	Control: The organization:	Y			
PE-10.01-01		PE-10.01-01	a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;	Y			
PE-10.01-02		PE-10.01-02	b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and	Y			
PE-10.01-03		PE-10.01-03	c. Protects emergency power shutoff capability from unauthorized activation.	Y			
		Supplemental Guidance	Supplemental Guidance: This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.	Y			
PE-10(1).01-00	Control Enhancements:	PE-10(1).01-00	(1) [Withdrawn: Incorporated into PE-10].	Y			
PE-11.01-00	PE-11 EMERGENCY POWER	PE-11.01-00	Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	Y			
		Supplemental Guidance	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	Y			
PE-11(1).01-01	Control Enhancements:	PE-11(1).01-01	(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	Y			
PE-11(1).01-02	Control Enhancements:	PE-11(1).01-02	(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.	Y			
		Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Long-term alternate power supplies for the information system are either manually or automatically activated.	Y			
PE-12.01-00	PE-12 EMERGENCY LIGHTING	PE-12.01-00	Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Y			
		Supplemental Guidance	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	Y			
PE-12(1).01-00	Control Enhancements:	PE-12(1).01-00	(1) The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.	Y			
PE-13.01-00	PE-13 FIRE PROTECTION	PE-13.01-00	Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	Y			
		Supplemental Guidance	Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security	Y			
PE-13(1).01-00	Control Enhancements:	PE-13(1).01-00	(1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.	Y			
PE-13(2).01-00	Control Enhancements:	PE-13(2).01-00	(2) The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.	Y			
PE-13(3).01-00	Control Enhancements:	PE-13(3).01-00	(3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	Y			
PE-13(4).01-00	Control Enhancements:	PE-13(4).01-00	(4) The organization ensures that the facility undergoes [*Assignment: organization-defined frequency*] fire marshal inspections and promptly resolves identified deficiencies.	Y			
PE-14.01-00	PE-14 TEMPERATURE AND HUMIDITY CONTROLS	PE-14.01-00	Control: The organization:	Y			
PE-14.01-01		PE-14.01-01	a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and	Y			
PE-14.01-02		PE-14.01-02	b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].	Y			
		Supplemental Guidance	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	Y			
PE-14(1).01-01	Control Enhancements:	PE-14(1).01-01	(1) The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.	Y			
PE-14(2).01-02	Control Enhancements:	PE-14(2).01-02	(2) The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.	Y			
PE-15.01-00	PE-15 WATER DAMAGE PROTECTION	PE-15.01-00	Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	Y			
		Supplemental Guidance	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	Y			

		PE-15(1).01-00	Control Enhancements:	PE-15(1).01-00	(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.	Y		
		PE-16.01-00	PE-16 DELIVERY AND REMOVAL	PE-16.01-00	Control: The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	Y		
				Supplemental Guidance	Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.	Y		
		PE-17.01-00	PE-17 ALTERNATE WORK SITE	PE-17.01-00	Control: The organization:	Y		
		PE-17.01-01		PE-17.01-01	a. Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites;	Y		
		PE-17.01-02		PE-17.01-02	c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Y		
		PE-17.01-03		PE-17.01-03	b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and	Y		
				Supplemental Guidance	Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.	Y		
		PE-18.01-00	PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS	PE-18.01-00	Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	Y		
				Supplemental Guidance	Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and	Y		
		PE-18(1).01-00	Control Enhancements:	PE-18(1).01-00	(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.	Y		
		PE-19.01-00	PE-19 INFORMATION LEAKAGE	PE-19.01-00	Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.	Y		
				Supplemental Guidance	Supplemental Guidance: The security categorization of the information system (with respect to confidentiality) and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.	Y		
						Y		
		PE-19(1).01-00	Control Enhancements:	PE-19(1).01-00	(1) The organization ensures that information system components, associated data communications, and networks are protected in accordance with: (i) national emissions and TEMPEST policies and procedures; and (ii) the sensitivity of the information being transmitted.	Y		
		PL-01.01-00	PL-1 SECURITY PLANNING POLICY AND PROCEDURES	PL-01.01-00	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:	Y		
		PL-01.01-01		PL-01.01-01	a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		PL-01.01-02		PL-01.01-02	b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards,	Y		
		PL-02.01-00	PL-2 SYSTEM SECURITY PLAN	PL-02.01-00	Control: The organization:	Y		
		PL-02.01-00		PL-02.01-00	a. Develops a security plan for the information system that:	Y		
		PL-02.01-01		PL-02.01-01	b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and	Y		
		PL-02.01-02		PL-02.01-02	c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	Y		
				Supplemental Guidance	Supplemental Guidance: The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational	Y		
						Y		
		PL-02(1).01-00	Control Enhancements:	PL-02(1).01-00	(1) The organization:	Y		
		PL-02(1).01-01	Control Enhancements:	PL-02(1).01-01	(a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and	Y		
		PL-02(1).01-02	Control Enhancements:	PL-02(1).01-02	(b) Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].	Y		
					Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.	Y		
		PL-02(2).01-00	Control Enhancements:	PL-02(2).01-00	(2) The organization develops a functional architecture for the information system that identifies and maintains:	Y		
		PL-02(2).01-01	Control Enhancements:	PL-02(2).01-01	(a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;	Y		
		PL-02(2).01-02	Control Enhancements:	PL-02(2).01-02	(b) User roles and the access privileges assigned to each role;	Y		
		PL-02(2).01-03	Control Enhancements:	PL-02(2).01-03	(c) Unique security requirements;	Y		
		PL-02(2).01-04	Control Enhancements:	PL-02(2).01-04	(d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and	Y		
		PL-02(2).01-05	Control Enhancements:	PL-02(2).01-05	(e) Restoration priority of information or information system services.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Unique security requirements for the information system include, for example, encryption of key data elements at rest. Specific protection needs for the information system include, for example, the Privacy Act and Health Insurance Portability and Accountability Act.	Y		
		PL-03.01-00	PL-3 SYSTEM SECURITY PLAN UPDATE	PL-03.01-00	[Withdrawn: Incorporated into PL-2].	Y		
		PL-04.01-00	PL-4 RULES OF BEHAVIOR	PL-04.01-00	Control: The organization:	Y		
		PL-04.01-01		PL-04.01-01	a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and	Y		

		PL-04.01-02		PL-04.01-02	b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	Y		
				Supplemental Guidance	Supplemental Guidance: The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior. Related control: PS-6.	Y		
		PL-04(1).01-00	Control Enhancements:	PL-04(1).01-00	(1) The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.	Y		
		PL-05.01-00	PL-5 PRIVACY IMPACT ASSESSMENT	PL-05.01-00	Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	Y		
		PL-06.01-00	PL-6 SECURITY-RELATED ACTIVITY PLANNING	PL-06.01-00	Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	Y		
				Supplemental Guidance	Supplemental Guidance: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.	Y		
		PS-01.01-00	PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES	PS-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		PS-01.01-01		PS-01.01-01	a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		PS-01.01-02		PS-01.01-02	b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards,	Y		
		PS-02.01-00	PS-2 POSITION CATEGORIZATION	PS-02.01-00	Control: The organization:	Y		
		PS-02.01-01		PS-02.01-01	a. Assigns a risk designation to all positions;	Y		
		PS-02.01-02		PS-02.01-02	b. Establishes screening criteria for individuals filling those positions; and	Y		
		PS-02.01-03		PS-02.01-03	c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	Y		
				Supplemental Guidance	Supplemental Guidance: Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).	Y		
		PS-03.01-00	PS-3 PERSONNEL SCREENING	PS-03.01-00	Control: The organization:	Y		
		PS-03.01-01		PS-03.01-01	a. Screens individuals prior to authorizing access to the information system; and	Y		
		PS-03.01-02		PS-03.01-02	b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].	Y		
				Supplemental Guidance	Supplemental Guidance: Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The organization may define different rescreening conditions and frequencies for personnel accessing the	Y		
		PS-03(1).01-00	Control Enhancements:	PS-03(1).01-00	(1) The organization ensures that every user accessing an information system processing, storing, or transmitting classified information is cleared and indoctrinated to the highest classification level of the information on the system.	Y		
		PS-03(2).01-00	Control Enhancements:	PS-03(2).01-00	(2) The organization ensures that every user accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, is formally indoctrinated for all of the relevant types of information on the system.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Types of information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI).	Y		
		PS-04.01-00	PS-4 PERSONNEL TERMINATION	PS-04.01-00	Control: The organization, upon termination of individual employment:	Y		
		PS-04.01-01		PS-04.01-01	a. Terminates information system access;	Y		
		PS-04.01-02		PS-04.01-02	b. Conducts exit interviews;	Y		
		PS-04.01-03		PS-04.01-03	c. Retrieves all security-related organizational information system-related property; and	Y		
		PS-04.01-04		PS-04.01-04	d. Retains access to organizational information and information systems formerly controlled by terminated individual.	Y		
				Supplemental Guidance	Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is	Y		
		PS-05.01-00	PS-5 PERSONNEL TRANSFER	PS-05.01-00	Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal*	Y		
				Supplemental Guidance	Supplemental Guidance: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer, whether permanent or temporary. Actions that may be required when personnel	Y		
		PS-06.01-00	PS-6 ACCESS AGREEMENTS	PS-06.01-00	Control: The organization:	Y		
		PS-06.01-01		PS-06.01-01	a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and	Y		
		PS-06.01-02		PS-06.01-02	b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].	Y		
				Supplemental Guidance	Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to	Y		
						Y		
		PS-06(1).01-00	Control Enhancements:	PS-06(1).01-00	(1) The organization ensures that access to information with special protection measures is granted only to individuals who:	Y		
		PS-06(1).01-01	Control Enhancements:	PS-06(1).01-01	(a) Have a valid access authorization that is demonstrated by assigned official government duties; and	Y		
		PS-06(1).01-02	Control Enhancements:	PS-06(1).01-02	(b) Satisfy associated personnel security criteria.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Information with special protection measures includes, for example, privacy information, proprietary information, and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.	Y		

		PS-06(2).01-00	Control Enhancements:	PS-06(2).01-00	(2) The organization ensures that access to classified information with special protection measures is granted only to individuals who:	Y		
		PS-06(2).01-01	Control Enhancements:	PS-06(2).01-01	(a) Have a valid access authorization that is demonstrated by assigned official government duties;	Y		
		PS-06(2).01-02	Control Enhancements:	PS-06(2).01-02	(b) Satisfy associated personnel security criteria consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and	Y		
		PS-06(2).01-03	Control Enhancements:	PS-06(2).01-03	(c) Have read, understand, and signed a nondisclosure agreement.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Examples of special protection measures include, for example, collateral, Special Access Program (SAP) and Sensitive Compartmented Information (SCI).	Y		
		PS-07.01-00	PS-7 THIRD-PARTY PERSONNEL SECURITY	PS-07.01-00	Control: The organization:	Y		
		PS-07.01-01		PS-07.01-01	a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;	Y		
		PS-07.01-02		PS-07.01-02	b. Documents personnel security requirements; and	Y		
		PS-07.01-03		PS-07.01-03	c. Monitors provider compliance.	Y		
				Supplemental Guidance	Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related	Y		
		PS-08.01-00	PS-8 PERSONNEL SANCTIONS	PS-08.01-00	Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	Y		
				Supplemental Guidance	Supplemental Guidance: The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization. Related controls: PL-4, PS-6.	Y		
		RA-01.01-00	RA-1 RISK ASSESSMENT POLICY AND PROCEDURES	RA-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		RA-01.01-01		RA-01.01-01	a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		RA-01.01-02		RA-01.01-02	b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards,	Y		
		RA-02.01-00	RA-2 SECURITY CATEGORIZATION	RA-02.01-00	Control: The organization:	Y		
		RA-02.01-01		RA-02.01-01	a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;	Y		
		RA-02.01-02		RA-02.01-02	b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and	Y		
		RA-02.01-03		RA-02.01-03	c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	Y		
				Supplemental Guidance	Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity,	Y		
		RA-03.01-00	RA-3 RISK ASSESSMENT	RA-03.01-00	Control: The organization:	Y		
		RA-03.01-01		RA-03.01-01	a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;	Y		
		RA-03.01-02		RA-03.01-02	b. Documents risk assessment results in [*Selection: security plan; risk assessment report*; [*Assignment: organization-defined document*]];	Y		
		RA-03.01-03		RA-03.01-03	c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and	Y		
		RA-03.01-04		RA-03.01-04	d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	Y		
				Supplemental Guidance	Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the	Y		
		RA-04.01-00	RA-4 RISK ASSESSMENT UPDATE	RA-04.01-00	[Withdrawn: Incorporated into RA-3].	Y		
		RA-05.01-00	RA-5 VULNERABILITY SCANNING	RA-05.01-00	Control: The organization:	Y		
		RA-05.01-01		RA-05.01-01	a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;	Y		
		RA-05.01-02		RA-05.01-02	b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:	Y		
		RA-05.01-03		RA-05.01-03	c. Analyzes vulnerability scan reports and results from security control assessments;	Y		
		RA-05.01-04		RA-05.01-04	d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and	Y		
		RA-05.01-05		RA-05.01-05	e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	Y		
				Supplemental Guidance	Supplemental Guidance: The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code	Y		
						Y		
		RA-05(1).01-00	Control Enhancements:	RA-05(1).01-00	(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	Y		
		RA-05(2).01-00	Control Enhancements:	RA-05(2).01-00	(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when new vulnerabilities are identified and reported.	Y		
		RA-05(3).01-00	Control Enhancements:	RA-05(3).01-00	(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).	Y		

	RA-05(4).01-00	Control Enhancements:	RA-05(4).01-00	(4) The organization attempts to discern what information about the information system is discoverable by adversaries.	Y		
	RA-05(5).01-00	Control Enhancements:	RA-05(5).01-00	(5) The organization includes privileged access authorization to [*Assignment: organization-identified information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning.	Y		
	RA-05(6).01-00	Control Enhancements:	RA-05(6).01-00	(6) The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.	Y		
	RA-05(7).01-00	Control Enhancements:	RA-05(7).01-00	(7) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.	Y		
	RA-05(8).01-00	Control Enhancements:	RA-05(8).01-00	(8) The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.	Y		
	RA-05(9).01-00	Control Enhancements:	RA-05(9).01-00	(9) The organization employs an independent penetration agent or penetration team to:	Y		
	RA-05(9).01-00	Control Enhancements:	RA-05(9).01-00	(a) Conduct a vulnerability analysis on the information system; and	Y		
	RA-05(9).01-00	Control Enhancements:	RA-05(9).01-00	(b) Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: A standard method for penetration testing includes: (i) pre-test analysis based on full knowledge of the target information system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of	Y		
	SA-01.01-00	SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	SA-01.01-00	Control: The organization: develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
	SA-01.01-01		SA-01.01-01	a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
	SA-01.01-02		SA-01.01-02	b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	Y		
			Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies,	Y		
	SA-02.01-00	SA-2 ALLOCATION OF RESOURCES	SA-02.01-00	Control: The organization:	Y		
	SA-02.01-01		SA-02.01-01	a. Includes a determination of information security requirements for the information system in mission/business process planning;	Y		
	SA-02.01-02		SA-02.01-02	b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and	Y		
	SA-02.01-03		SA-02.01-03	c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	Y		
	SA-03.01-00	SA-3 LIFE CYCLE SUPPORT	SA-03.01-00	Control: The organization:	Y		
	SA-03.01-01		SA-03.01-01	a. Manages the information system using a system development life cycle methodology that includes information security considerations;	Y		
	SA-03.01-02		SA-03.01-02	b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and	Y		
	SA-03.01-03		SA-03.01-03	c. Identifies individuals having information system security roles and responsibilities.	Y		
	SA-04.01-00	SA-4 ACQUISITIONS	SA-04.01-00	Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:	Y		
	SA-04.01-01		SA-04.01-01	a. Security functional requirements/specifications;	Y		
	SA-04.01-02		SA-04.01-02	b. Security-related documentation requirements; and	Y		
	SA-04.01-03		SA-04.01-03	c. Developmental and evaluation-related assurance requirements.	Y		
			Supplemental Guidance	Supplemental Guidance: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA	Y		
	SA-04(1).01-00	Control Enhancements:	SA-04(1).01-00	(1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.	Y		
	SA-04(2).01-00	Control Enhancements:	SA-04(2).01-00	(2) The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in	Y		
	SA-04(3).01-00	Control Enhancements:	SA-04(3).01-00	(3) The organization requires software vendors/manufacturers to demonstrate that their software development processes employ state-of-the-practice software and security engineering methods, quality control processes, and validation techniques to minimize flawed or malformed software.	Y		
	SA-04(4).01-00	Control Enhancements:	SA-04(4).01-00	(4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	Y		
	SA-04(5).01-00	Control Enhancements:	SA-04(5).01-00	(5) The organization requires in acquisition documents, that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.	Y		
	SA-04(6).01-00	Control Enhancements:	SA-04(6).01-00	(6) The organization:	Y		
	SA-04(6).01-01	Control Enhancements:	SA-04(6).01-01	(a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that composes an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being	Y		
	SA-04(6).01-02	Control Enhancements:	SA-04(6).01-02	(b) Ensures that these products have been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: COTS IA or IA-enabled information technology products used to protect classified information by cryptographic means, may be required to use NSA-approved key management.	Y		
	SA-04(7).01-00	Control Enhancements:	SA-04(7).01-00	(7) The organization:	Y		
	SA-04(7).01-01	Control Enhancements:	SA-04(7).01-01	(a) Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists; and	Y		
	SA-04(7).01-02	Control Enhancements:	SA-04(7).01-02	(b) Requires, if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.	Y		
	SA-05.01-00	SA-5 INFORMATION SYSTEM DOCUMENTATION	SA-05.01-00	Control: The organization:	Y		

		SA-05.01-01		SA-05.01-01	a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:	Y		
		SA-05.01-02		SA-05.01-02	b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:	Y		
		SA-05.01-03		SA-05.01-03	c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	Y		
				Supplemental Guidance	Supplemental Guidance: The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to	Y		
						Y		
		SA-05(1).01-00	Control Enhancements:	SA-05(1).01-00	(1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.	Y		
		SA-05(2).01-00	Control Enhancements:	SA-05(2).01-00	(2) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.	Y		
		SA-05(3).01-00	Control Enhancements:	SA-05(3).01-00	(3) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.	Y		
		SA-05(4).01-00	Control Enhancements:	SA-05(4).01-00	(4) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Each subsystem within an information system can contain one or more modules.	Y		
		SA-05(5).01-00	Control Enhancements:	SA-05(5).01-00	(5) The organization obtains, protects as required, and makes available to authorized personnel, the source code for the information system to permit analysis and testing.	Y		
		SA-06.01-00	SA-6 SOFTWARE USAGE RESTRICTIONS	SA-06.01-00	Control: The organization:	Y		
		SA-06.01-01		SA-06.01-01	a. Uses software and associated documentation in accordance with contract agreements and copyright laws;	Y		
		SA-06.01-02		SA-06.01-02	b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and	Y		
		SA-06.01-03		SA-06.01-03	c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Y		
				Supplemental Guidance	Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.	Y		
		SA-06(1).01-00	Control Enhancements:	SA-06(1).01-00	(1) The organization:	Y		
		SA-06(1).01-01		SA-06(1).01-01	(a) Prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code; and	Y		
		SA-06(1).01-02		SA-06(1).01-02	(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Software products without accompanying source code from sources with limited or no warranty are assessed for potential security impacts. The assessment addresses the fact that these types of software products are difficult or impossible to review, repair, or extend, given that the organization does not have access to	Y		
		SA-07.01-00	SA-7 USER-INSTALLED SOFTWARE	SA-07.01-00	Control: The organization enforces explicit rules governing the installation of software by users.	Y		
				Supplemental Guidance	Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is	Y		
		SA-08.01-00	SA-8 SECURITY ENGINEERING PRINCIPLES	SA-08.01-00	Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Y		
				Supplemental Guidance	Supplemental Guidance: The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and	Y		
		SA-09.01-00	SA-9 EXTERNAL INFORMATION SYSTEM SERVICES	SA-09.01-00	Control: The organization:	Y		
		SA-09.01-01		SA-09.01-01	a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;	Y		
		SA-09.01-02		SA-09.01-02	b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and	Y		
		SA-09.01-03		SA-09.01-03	c. Monitors security control compliance by external service providers.	Y		
				Supplemental Guidance	Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for	Y		
		SA-09(1).01-00	Control Enhancements:	SA-09(1).01-00	(1) The organization:	Y		
		SA-09(1).01-01	Control Enhancements:	SA-09(1).01-01	(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and	Y		
		SA-09(1).01-02	Control Enhancements:	SA-09(1).01-02	(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined senior organizational official*].	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.	Y		
		SA-10.01-00	SA-10 DEVELOPER CONFIGURATION MANAGEMENT	SA-10.01-00	Control: The organization requires that information system developers/integrators:	Y		
		SA-10.01-01		SA-10.01-01	a. Perform configuration management during information system design, development, implementation, and operation;	Y		
		SA-10.01-02		SA-10.01-02	b. Manage and control changes to the information system;	Y		
		SA-10.01-03		SA-10.01-03	c. Implement only organization-approved changes;	Y		
		SA-10.01-04		SA-10.01-04	d. Document approved changes to the information system; and	Y		

	SA-10.01-05		SA-10.01-05	e. Track security flaws and flaw resolution.	Y		
				Supplemental Guidance: Related controls: CM-3, CM-4, CM-9.	Y		
	SA-10(1).01-00	Control Enhancements:	SA-10(1).01-00	(1) The organization requires that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery.	Y		
	SA-10(2).01-00	Control Enhancements:	SA-10(2).01-00	(2) The organization provides an alternative configuration management process with organizational personnel in the absence of dedicated developer/integrator configuration management team.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The configuration management process includes key organizational personnel that are responsible for reviewing and approving proposed changes to the information system, and security personnel that conduct impact analyses prior to the implementation of any changes to the system.	Y		
	SA-11.01-00	SA-11 DEVELOPER SECURITY TESTING	SA-11.01-00	Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):	Y		
	SA-11.01-01		SA-11.01-01	a. Create and implement a security test and evaluation plan;	Y		
	SA-11.01-02		SA-11.01-02	b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and	Y		
	SA-11.01-03		SA-11.01-03	c. Document the results of the security testing/evaluation and flaw remediation processes.	Y		
			Supplemental Guidance	Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security	Y		
	SA-11(1).01-00	Control Enhancements:	SA-11(1).01-00	(1) The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.	Y		
	SA-11(2).01-00	Control Enhancements:	SA-11(2).01-00	(2) The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.	Y		
	SA-11(3).01-00	Control Enhancements:	SA-11(3).01-00	(3) The organization requires that information system developers/integrators create a security test and evaluation plan and implement the plan under the witness of an independent verification and validation agent.	Y		
	SA-12.01-00	SA-12 SUPPLY CHAIN PROTECTION	SA-12.01-00	Control: The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*] as part of a comprehensive, defense-in-breadth information security strategy.	Y		
			Supplemental Guidance	Supplemental Guidance: A defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations,	Y		
	SA-12(1).01-00	Control Enhancements:	SA-12(1).01-00	(1) The organization purchases all anticipated information system components and spares in the initial acquisition.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Stockpiling information system components and spares avoids the need to use less trustworthy secondary or resale markets in future years.	Y		
	SA-12(2).01-00	Control Enhancements:	SA-12(2).01-00	(2) The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The organization reviews supplier claims with regard to the use of appropriate security processes in the development and manufacture of information system components or products.	Y		
	SA-12(3).01-00	Control Enhancements:	SA-12(3).01-00	(3) The organization uses trusted shipping and warehousing for information systems, information system components, and information technology products.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Trusted shipping and warehousing reduces opportunities for subversive activities or interception during transit. Examples of supporting techniques include the use of a geographically aware beacon to detect shipment diversions or delays. Related control: PE-16.	Y		
	SA-12(4).01-00	Control Enhancements:	SA-12(4).01-00	(4) The organization employs a diverse set of suppliers for information systems, information system components, information technology products, and information system services.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Diversification of suppliers is intended to limit the potential harm from a given supplier in a supply chain, increasing the work factor for an adversary.	Y		
	SA-12(5).01-00	Control Enhancements:	SA-12(5).01-00	(5) The organization employs standard configurations for information systems, information system components, and information technology products..	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: By avoiding the purchase of custom configurations for information systems, information system components, and information technology products, the organization limits the possibility of acquiring systems and products that have been corrupted via the supply chain actions targeted at the organization.	Y		
	SA-12(6).01-00	Control Enhancements:	SA-12(6).01-00	(6) The organization minimizes the time between purchase decisions and delivery of information systems, information system components, and information technology products.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: By minimizing the time between purchase decisions and required delivery of information systems, information system components, and information technology products, the organization limits the opportunity for an adversary to corrupt the purchased system, component, or product.	Y		
	SA-12(7).01-00	Control Enhancements:	SA-12(7).01-00	(7) The organization employs independent analysis and penetration testing against delivered information systems, information system components, and information technology products.	Y		
	SA-13.01-00	SA-13 TRUSTWORTHINESS	SA-13.01-00	Control: The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].	Y		
	SA-14.01-00	SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS	SA-14.01-00	Control: The organization:	Y		
	SA-14.01-01		SA-14.01-01	a. Determines [*Assignment: organization-defined list of critical information system components that require re-implementation*]; and	Y		
	SA-14.01-02		SA-14.01-02	b. Re-implements or custom develops such information system components.	Y		
			Supplemental Guidance	Supplemental Guidance: The underlying assumption is that the list of information technology products defined by the organization cannot be trusted due to threats from the supply chain that the organization finds unacceptable. The organization re-implements or custom develops such components to satisfy requirements for high assurance. Related	Y		
	SA-14(1).01-00	Control Enhancements:	SA-14(1).01-00	(1) The organization:	Y		
	SA-14(1).01-01	Control Enhancements:	SA-14(1).01-01	(a) Identifies information system components for which alternative sourcing is not viable; and	Y		
	SA-14(1).01-02	Control Enhancements:	SA-14(1).01-02	(b) Employs [*Assignment: organization-defined measures*] to ensure that critical security controls for the information system components are not compromised.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Measures that the organization considers implementing include, for example, enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.	Y		
	SC-01.01-00	SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	SC-01.01-00	Control: The organization develops, documents, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
	SC-01.01-01		SC-01.01-01	a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		

		SC-01.01-02		SC-01.01-02	b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies,	Y		
		SC-02.01-00	SC-2 APPLICATION PARTITIONING	SC-02.01-00	Control: The information system separates user functionality (including user interface services) from information system management functionality.	Y		
				Supplemental Guidance	Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is	Y		
		SC-02(1).01-00	Control Enhancements:	SC-02(1).01-00	(1) The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The intent of this control enhancement is to ensure that administration options are not available to general users (including prohibiting the use of the grey-out option commonly used to eliminate accessibility to such information). For example, administration options are not presented until the user has appropriately	Y		
		SC-03.01-00	SC-3 SECURITY FUNCTION ISOLATION	SC-03.01-00	Control: The information system isolates security functions from nonsecurity functions.	Y		
				Supplemental Guidance	Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a	Y		
		SC-03(1).01-00	Control Enhancements:	SC-03(1).01-00	(1) The information system implements underlying hardware separation mechanisms to facilitate security function isolation.	Y		
		SC-03(2).01-00	Control Enhancements:	SC-03(2).01-00	(2) The information system isolates security functions enforcing access and information flow control from both nonsecurity functions and from other security functions.	Y		
		SC-03(3).01-00	Control Enhancements:	SC-03(3).01-00	(3) The organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Nonsecurity functions contained within the isolation boundary are considered security-relevant.	Y		
		SC-03(4).01-00		SC-03(4).01-00	(4) The organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.	Y		
		SC-03(5).01-00		SC-03(5).01-00	(5) The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	Y		
		SC-04.01-00	SC-4 INFORMATION IN SHARED RESOURCES	SC-04.01-00	Control: The information system prevents unauthorized and unintended information transfer via shared system resources.	Y		
				Supplemental Guidance	Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource	Y		
		SC-04(1).01-00	Control Enhancements:	SC-04(1).01-00	(1) The information system does not share resources that are used to interface with systems operating at different security levels.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Shared resources include, for example, memory, input/output queues, and network interface cards.	Y		
		SC-05.01-00	SC-5 DENIAL OF SERVICE PROTECTION	SC-05.01-00	Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].	Y		
				Supplemental Guidance	Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and	Y		
		SC-05(1).01-00	Control Enhancements:	SC-05(1).01-00	(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.	Y		
		SC-05(2).01-00	Control Enhancements:	SC-05(2).01-00	(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	Y		
		SC-06.01-00	SC-6 RESOURCE PRIORITY	SC-06.01-00	Control: The information system limits the use of resources by priority.	Y		
				Supplemental Guidance	Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. This control does not apply to components in the information system for which there is only a single user/role.	Y		
		SC-07.01-00	SC-7 BOUNDARY PROTECTION	SC-07.01-00	Control: The information system:	Y		
		SC-07.01-01		SC-07.01-01	a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and	Y		
		SC-07.01-02		SC-07.01-02	b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Y		
				Supplemental Guidance	Supplemental Guidance: Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example,	Y		
				Supplemental Guidance	The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial	Y		
		SC-07(1).01-00	Control Enhancements:	SC-07(1).01-00	(1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.	Y		
		SC-07(2).01-00	Control Enhancements:	SC-07(2).01-00	(2) The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	Y		
		SC-07(3).01-00	Control Enhancements:	SC-07(3).01-00	(3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.	Y		
		SC-07(4).01-00	Control Enhancements:	SC-07(4).01-00	(4) The organization:	Y		
		SC-07(4).01-01	Control Enhancements:	SC-07(4).01-01	(a) Implements a managed interface for each external telecommunication service;	Y		
		SC-07(4).01-02	Control Enhancements:	SC-07(4).01-02	(b) Establishes a traffic flow policy for each managed interface;	Y		
		SC-07(4).01-03	Control Enhancements:	SC-07(4).01-03	(c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;	Y		
		SC-07(4).01-04	Control Enhancements:	SC-07(4).01-04	(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;	Y		

	SC-07(4).01-05	Control Enhancements:	SC-07(4).01-05	(e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]; and	Y		
	SC-07(4).01-06	Control Enhancements:	SC-07(4).01-06	(f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.	Y		
	SC-07(5).01-00	Control Enhancements:	SC-07(5).01-00	(5) The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	Y		
	SC-07(6).01-00	Control Enhancements:	SC-07(6).01-00	(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	Y		
	SC-07(7).01-00	Control Enhancements:	SC-07(7).01-00	(7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is	Y		
	SC-07(8).01-00	Control Enhancements:	SC-07(8).01-00	(8) The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: External networks are networks outside the control of the organization. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Proxy servers are also configurable with	Y		
	SC-07(9).01-00	Control Enhancements:	SC-07(9).01-00	(9) The information system, at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Detecting internal actions that may pose a security threat to external information systems is sometimes termed extrusion detection. Extrusion detection at the information system boundary includes the analysis of network traffic (incoming as well as outgoing) looking for indications of an internal threat to the	Y		
	SC-07(10).01-00	Control Enhancements:	SC-07(10).01-00	(10) The organization prevents the unauthorized exfiltration of information across managed interfaces.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Measures to prevent unauthorized exfiltration of information from the information system include, for example: (i) strict adherence to protocol formats; (ii) monitoring for indications of beaconing from the information system; (iii) monitoring for use of steganography; (iv) disconnecting external network interfaces	Y		
	SC-07(11).01-00	Control Enhancements:	SC-07(11).01-00	(11) The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.	Y		
	SC-07(12).01-00	Control Enhancements:	SC-07(12).01-00	(12) The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.	Y		
	SC-07(13).01-00	Control Enhancements:	SC-07(13).01-00	(13) The organization isolates [*Assignment: organization defined key information security tools, mechanisms, and support components*] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.	Y		
	SC-07(14).01-00	Control Enhancements:	SC-07(14).01-00	(14) The organization protects against unauthorized physical connections across the boundary protections implemented at [*Assignment: organization-defined list of managed interfaces*].	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Information systems operating at different security categories may routinely share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets,	Y		
	SC-07(15).01-00	Control Enhancements:	SC-07(15).01-00	(15) The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Related controls: AC-2, AC-3, AC-4, AU-2.	Y		
	SC-07(16).01-00	Control Enhancements:	SC-07(16).01-00	(16) The information system prevents discovery of specific system components (or devices) composing a managed interface.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement is intended to protect the network addresses of information system components that are part of the managed interface from discovery through common tools and techniques used to identify devices on a network. The network addresses are not available for discovery (e.g., not published or	Y		
	SC-07(17).01-00	Control Enhancements:	SC-07(17).01-00	(17) The organization employs automated mechanisms to enforce strict adherence to protocol format.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Automated mechanisms used to enforce protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification (e.g., IEEE) at the application layer and serve to identify significant vulnerabilities that cannot be detected by devices	Y		
	SC-07(18).01-00	Control Enhancements:	SC-07(18).01-00	(18) The information system fails securely in the event of an operational failure of a boundary protection device.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Fail secure is a condition achieved by the application of a set of information system mechanisms to ensure that in the event of an operational failure of a boundary protection device at a managed interface (e.g., router, firewall, guard, application gateway residing on a protected subnetwork commonly	Y		
	SC-08.01-00	SC-8 TRANSMISSION INTEGRITY	SC-08.01-00	Control: The information system protects the integrity of transmitted information.	Y		
			Supplemental Guidance	Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of	Y		
	SC-08(1).01-00	Control Enhancements:	SC-08(1).01-00	(1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.	Y		
	SC-08(2).01-00	Control Enhancements:	SC-08(2).01-00	(2) The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously modified at data aggregation or protocol transformation points, compromising the integrity of the information.	Y		
	SC-09.01-00	SC-9 TRANSMISSION CONFIDENTIALITY	SC-09.01-00	Control: The information system protects the confidentiality of transmitted information.	Y		
			Supplemental Guidance	Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of	Y		
	SC-09(1).01-00	Control Enhancements:	SC-09(1).01-00	(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.	Y		
	SC-09(2).01-00		SC-09(2).01-00	(2) The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously disclosed at data aggregation or protocol transformation points, compromising the confidentiality of the information.	Y		
	SC-10.01-00	SC-10 NETWORK DISCONNECT	SC-10.01-00	Control: The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.	Y		

					Supplemental Guidance	Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application	Y			
			SC-11.01-00	SC-11 TRUSTED PATH	SC-11.01-00	Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].	Y			
					Supplemental Guidance	Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).	Y			
			SC-12.01-00	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12.01-00	Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	Y			
					Supplemental Guidance	Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the	Y			
							Y			
			SC-12(1).01-00	Control Enhancements:	SC-12(1).01-00	(1) The organization maintains availability of information in the event of the loss of cryptographic keys by users.	Y			
			SC-12(2).01-00	Control Enhancements:	SC-12(2).01-00	(2) The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST-approved, NSA-approved*] key management technology and processes.	Y			
			SC-12(3).01-00	Control Enhancements:	SC-12(3).01-00	(3) The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using NSA-approved key management technology and processes.	Y			
			SC-12(4).01-00	Control Enhancements:	SC-12(4).01-00	(4) The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material.	Y			
			SC-12(5).01-00	Control Enhancements:	SC-12(5).01-00	(5) The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.	Y			
			SC-13.01-00	SC-13 USE OF CRYPTOGRAPHY	SC-13.01-00	Control: The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	Y			
			SC-13(1).01-00	Control Enhancements:	SC-13(1).01-00	(1) The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.	Y			
			SC-13(2).01-00	Control Enhancements:	SC-13(2).01-00	(2) The organization employs NSA-approved cryptography to protect classified information.	Y			
			SC-13(3).01-00	Control Enhancements:	SC-13(3).01-00	(3) The organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.	Y			
			SC-13(4).01-00	Control Enhancements:	SC-13(4).01-00	(4) The organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.	Y			
			SC-14.01-00	SC-14 PUBLIC ACCESS PROTECTIONS	SC-14.01-00	Control: The information system protects the integrity and availability of publicly available information and applications.	Y			
					Supplemental Guidance	Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.	Y			
			SC-15.01-00	SC-15 COLLABORATIVE COMPUTING DEVICES	SC-15.01-00	Control: The information system:	Y			
			SC-15.01-00		SC-15.01-00	a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and	Y			
			SC-15.01-00		SC-15.01-00	b. Provides an explicit indication of use to users physically present at the devices.	Y			
					Supplemental Guidance	Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.	Y			
			SC-15(1).01-00	Control Enhancements:	SC-15(1).01-00	(1) The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.	Y			
			SC-15(2).01-00	Control Enhancements:	SC-15(2).01-00	(2) The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.	Y			
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Blocking restrictions do not include instant messaging services that are configured by an organization to perform an authorized function.	Y			
			SC-15(3).01-00	Control Enhancements:	SC-15(3).01-00	(3) The organization disables or removes collaborative computing devices from information systems in [*Assignment: organization-defined secure work areas*].	Y			
			SC-16.01-00	SC-16 TRANSMISSION OF SECURITY ATTRIBUTES	SC-16.01-00	Control: The information system associates security attributes with information exchanged between information systems.	Y			
					Supplemental Guidance	Supplemental Guidance: Security attributes may be explicitly or implicitly associated with the information contained within the information system. Related control: AC-16.	Y			
							Y			
			SC-16(1).01-00	Control Enhancements:	SC-16(1).01-00	(1) The information system validates the integrity of security attributes exchanged between systems.	Y			
			SC-17.01-00	SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17.01-00	Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	Y			
					Supplemental Guidance	Supplemental Guidance: For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice.	Y			
			SC-18.01-00	SC-18 MOBILE CODE	SC-18.01-00	Control: The organization:	Y			
			SC-18.01-01		SC-18.01-01	a. Defines acceptable and unacceptable mobile code and mobile code technologies;	Y			
			SC-18.01-02		SC-18.01-02	b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and	Y			
			SC-18.01-03		SC-18.01-03	c. Authorizes, monitors, and controls the use of mobile code within the information system.	Y			
					Supplemental Guidance	Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript.	Y			
			SC-18(1).01-00	Control Enhancements:	SC-18(1).01-00	(1) The information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.	Y			
					Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Corrective actions when unauthorized mobile code is detected include, for example, blocking, quarantine, or alerting administrator. Disallowed transfers include, for example, sending word processing files with embedded macros.	Y			

	SC-18(2).01-00		SC-18(2).01-00	(2) The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [*Assignment: organization-defined mobile code requirements*].	Y		
	SC-18(3).01-00		SC-18(3).01-00	(3) The information system prevents the download and execution of prohibited mobile code.	Y		
	SC-18(4).01-00		SC-18(4).01-00	(4) The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and requires [*Assignment: organization-defined actions*] prior to executing the code.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Actions required before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments.	Y		
	SC-19.01-00	SC-19 VOICE OVER INTERNET PROTOCOL	SC-19.01-00	Control: The organization:	Y		
	SC-19.01-01		SC-19.01-01	a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and	Y		
	SC-19.01-02		SC-19.01-02	b. Authorizes, monitors, and controls the use of VoIP within the information system.	Y		
	SC-20.01-00	SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	SC-20.01-00	Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.	Y		
			Supplemental Guidance	Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service.	Y		
					Y		
	SC-20(1).01-00	Control Enhancements:	SC-20(1).01-00	(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	Y		
				Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.	Y		
					Y		
	SC-21.01-00	SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	SC-21.01-00	Control: The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.	Y		
			Supplemental Guidance	Supplemental Guidance: A recursive resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS servers are examples of authoritative sources. Information systems that use technologies other than the DNS to map between host/service	Y		
					Y		
	SC-21(1).01-00	Control Enhancements:	SC-21(1).01-00	(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.	Y		
	SC-22.01-00	SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	SC-22.01-00	Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Y		
			Supplemental Guidance	Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary.	Y		
	SC-23.01-00	SC-23 SESSION AUTHENTICITY	SC-23.01-00	Control: The information system provides mechanisms to protect the authenticity of communications sessions.	Y		
			Supplemental Guidance	Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-	Y		
	SC-23(1).01-00	Control Enhancements:	SC-23(1).01-00	(1) The information system invalidates session identifiers upon user logout or other session termination.	Y		
	SC-23(2).01-00	Control Enhancements:	SC-23(2).01-00	(2) The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.	Y		
	SC-23(3).01-00	Control Enhancements:	SC-23(3).01-00	(3) The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.	Y		
	SC-23(4).01-00	Control Enhancements:	SC-23(4).01-00	(4) The information system generates unique session identifiers with [*Assignment: organization-defined randomness requirements*].	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers.	Y		
	SC-24.01-00	SC-24 FAIL IN KNOWN STATE	SC-24.01-00	Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.	Y		
			Supplemental Guidance	Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps	Y		
	SC-25.01-00	SC-25 THIN NODES	SC-25.01-00	Control: The information system employs processing components that have minimal functionality and information storage.	Y		
			Supplemental Guidance	Supplemental Guidance: The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack. Related control: SC-30.	Y		
	SC-26.01-00	SC-26 HONEYPOTS	SC-26.01-00	Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.	Y		
	SC-26(1).01-00		SC-26(1).01-00	(1) The information system includes components that proactively seek to identify web-based malicious code.	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Devices that actively seek out web-based malicious code by posing as clients are referred to as client honeypots or honey clients.	Y		
	SC-27.01-00	SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS	SC-27.01-00	Control: The information system includes: [*Assignment: organization-defined operating system-independent applications*].	Y		
			Supplemental Guidance	Supplemental Guidance: Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while information systems with a given operating	Y		
	SC-28.01-00	SC-28 PROTECTION OF INFORMATION AT REST	SC-28.01-00	Control: The information system protects the confidentiality and integrity of information at rest.	Y		
			Supplemental Guidance	Supplemental Guidance: This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information	Y		
	SC-28(1).01-00	Control Enhancements:	SC-28(1).01-00	(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.	Y		

		SC-29.01-00	SC-29 HETEROGENEITY	SC-29.01-00	Control: The organization employs diverse information technologies in the implementation of the information system.	Y		
				Supplemental Guidance	Supplemental Guidance: Increasing the diversity of information technologies within the information system reduces the impact of the exploitation of a specific technology. Organizations that select overhead, both of which have the potential to lead to mistakes and misconfigurations which could increase overall risk.	Y		
		SC-30.01-00	SC-30 VIRTUALIZATION TECHNIQUES	SC-30.01-00	Control: The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.	Y		
				Supplemental Guidance	Supplemental Guidance: Virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.	Y		
		SC-30(1).01-00	Control Enhancements:	SC-30(1).01-00	(1) The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes result in an increased work factor for adversaries in order to carry out successful attacks. Changing the apparent operating system or application, as opposed to the actual operating system or	Y		
		SC-30(2).01-00	Control Enhancements:	SC-30(2).01-00	(2) The organization employs randomness in the implementation of the virtualization techniques.	Y		
		SC-31.01-00	SC-31 COVERT CHANNEL ANALYSIS	SC-31.01-00	Control: The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.	Y		
				Supplemental Guidance	Supplemental Guidance: Information system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information	Y		
		SC-31(1).01-00	Control Enhancements:	SC-31(1).01-00	(1) The organization tests a subset of the vendor-identified covert channel avenues to determine if they are exploitable.	Y		
		SC-32.01-00	SC-32 INFORMATION SYSTEM PARTITIONING	SC-32.01-00	Control: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	Y		
				Supplemental Guidance	Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain	Y		
		SC-33.01-00	SC-33 TRANSMISSION PREPARATION INTEGRITY	SC-33.01-00	Control: The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.	Y		
				Supplemental Guidance	Supplemental Guidance: Information can be subjected to unauthorized changes (e.g., malicious and/or unintentional modification) at information aggregation or protocol transformation points.	Y		
		SC-34.01-00	SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS	SC-34.01-00	Control: The information system at [*Assignment: organization-defined information system components*]:	Y		
		SC-34.01-01		SC-34.01-01	a. Loads and executes the operating environment from hardware-enforced, read-only media; and	Y		
		SC-34.01-02		SC-34.01-02	b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.	Y		
				Enhanced Supplemental Guidance	Supplemental Guidance: In this control, the term operating environment is defined as the code upon which applications are hosted, for example, a monitor, executive, operating system, or application running directly on the hardware platform. Hardware-enforced, read-only media include, for example, CD-R/DVD-R disk drives. Use of non-modifiable	Y		
		SC-34(1).01-00	Control Enhancements:	SC-34(1).01-00	(1) The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.	Y		
					Enhancement Supplemental Guidance: This control enhancement: (i) eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system component; and (ii) requires no such removable storage be employed, a requirement that may be applied directly or as a specific restriction imposed through	Y		
		SC-34(2).01-00	Control Enhancements:	SC-34(2).01-00	(2) The organization protects the integrity of the information on read-only media.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: This control enhancement covers protecting the integrity of information to be placed onto read-only media and controlling the media after information has been recorded onto the media. Protection measures may include, as deemed necessary by the organization, a combination of prevention and detection/response.	Y		
		SI-01.01-00	SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	SI-01.01-00	Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	Y		
		SI-01.01-01		SI-01.01-01	a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Y		
		SI-01.01-02		SI-01.01-02	b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	Y		
				Supplemental Guidance	Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies,	Y		
		SI-02.01-00	SI-2 FLAW REMEDIATION	SI-02.01-00	Control: The organization:	Y		
		SI-02.01-01		SI-02.01-01	a. Identifies, reports, and corrects information system flaws;	Y		
		SI-02.01-02		SI-02.01-02	b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and	Y		
		SI-02.01-03		SI-02.01-03	c. Incorporates flaw remediation into the organizational configuration management process.	Y		
				Supplemental Guidance	Supplemental Guidance: The organization identifies information systems containing software affected by recently announced-software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information	Y		
						Y		
		SI-02(1).01-00	Control Enhancements:	SI-02(1).01-00	(1) The organization centrally manages the flaw remediation process and installs software updates automatically.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.	Y		
		SI-02(2).01-00	Control Enhancements:	SI-02(2).01-00	(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.	Y		
		SI-02(3).01-00	Control Enhancements:	SI-02(3).01-00	(3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].	Y		
		SI-02(4).01-00	Control Enhancements:	SI-02(4).01-00	(4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].	Y		
		SI-03.01-00	SI-3 MALICIOUS CODE PROTECTION	SI-03.01-00	Control: The organization:	Y		
		SI-03.01-01		SI-03.01-01	a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;	Y		

SI-03.01-02		SI-03.01-02	b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;	Y			
SI-03.01-03		SI-03.01-03	c. Configures malicious code protection mechanisms to: Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources as the files are downloaded,	Y			
SI-03.01-04		SI-03.01-04	d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	Y			
		Supplemental Guidance	Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained	Y			
SI-03(1).01-00	Control Enhancements:	SI-03(1).01-00	(1) The organization centrally manages malicious code protection mechanisms.	Y			
SI-03(2).01-00	Control Enhancements:	SI-03(2).01-00	(2) The information system automatically updates malicious code protection mechanisms (including signature definitions).	Y			
SI-03(3).01-00	Control Enhancements:	SI-03(3).01-00	(3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.	Y			
SI-03(4).01-00	Control Enhancements:	SI-03(4).01-00	(4) The information system updates malicious code protection mechanisms only when directed by a privileged user.	Y			
SI-03(5).01-00	Control Enhancements:	SI-03(5).01-00	(5) The organization does not allow users to introduce removable media into the information system.	Y			
SI-03(6).01-00	Control Enhancements:	SI-03(6).01-00	(6) The organization tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.	Y			
SI-04.01-00	SI-4 INFORMATION SYSTEM MONITORING	SI-04.01-00	Control: The organization:	Y			
SI-04.01-01		SI-04.01-01	a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks;	Y			
SI-04.01-02		SI-04.01-02	b. Identifies unauthorized use of the information system;	Y			
SI-04.01-03		SI-04.01-03	c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;	Y			
SI-04.01-04		SI-04.01-04	d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and	Y			
SI-04.01-05		SI-04.01-05	e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	Y			
		Supplemental Guidance	Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal	Y			
SI-04(1).01-00	Control Enhancements:	SI-04(1).01-00	(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.	Y			
SI-04(2).01-00	Control Enhancements:	SI-04(2).01-00	(2) The organization employs automated tools to support near real-time analysis of events.	Y			
SI-04(3).01-00	Control Enhancements:	SI-04(3).01-00	(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.	Y			
SI-04(4).01-00	Control Enhancements:	SI-04(4).01-00	(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	Y			
		Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code	Y			
SI-04(5).01-00	Control Enhancements:	SI-04(5).01-00	(5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].	Y			
		Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.	Y			
SI-04(6).01-00	Control Enhancements:	SI-04(6).01-00	(6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	Y			
SI-04(7).01-00	Control Enhancements:	SI-04(7).01-00	(7) The information system notifies [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role)*] of suspicious events and takes [*Assignment: organization-defined list of least-disruptive actions to terminate suspicious events*].	Y			
		Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The least-disruptive actions may include initiating a request for human response.	Y			
SI-04(8).01-00	Control Enhancements:	SI-04(8).01-00	(8) The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.	Y			
SI-04(9).01-00	Control Enhancements:	SI-04(9).01-00	(9) The organization tests/exercises intrusion-monitoring tools [*Assignment: organization-defined time-period*].	Y			
		Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The frequency of testing/exercises is dependent upon the type and method of deployment of the intrusion-monitoring tools.	Y			
SI-04(10).01-00	Control Enhancements:	SI-04(10).01-00	(10) The organization makes provisions so that encrypted traffic is visible to information system monitoring tools.	Y			
		Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: The enhancement recognizes the need to balance encrypting traffic versus the need to have insight into that traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of traffic is paramount; for others, the mission-assurance concerns are greater.	Y			
SI-04(11).01-00	Control Enhancements:	SI-04(11).01-00	(11) The organization analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.	Y			
		Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Anomalies within the information system include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.	Y			
SI-04(12).01-00	Control Enhancements:	SI-04(12).01-00	(12) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts*].	Y			
SI-04(13).01-00	Control Enhancements:	SI-04(13).01-00	(13) The organization:	Y			
SI-04(13).01-01	Control Enhancements:	SI-04(13).01-01	(a) Analyzes communications traffic/event patterns for the information system;	Y			
SI-04(13).01-02	Control Enhancements:	SI-04(13).01-02	(b) Develops profiles representing common traffic patterns and/or events; and	Y			
SI-04(13).01-03	Control Enhancements:	SI-04(13).01-03	(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to [*Assignment: organization-defined measure of false positives*] and the number of false negatives to [*Assignment: organization-defined measure of false negatives*].	Y			

		SI-04(14).01-00	Control Enhancements:	SI-04(14).01-00	(14) The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	Y		
		SI-04(15).01-00	Control Enhancements:	SI-04(15).01-00	(15) The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	Y		
		SI-04(16).01-00	Control Enhancements:	SI-04(16).01-00	(16) The organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.	Y		
		SI-04(17).01-00	Control Enhancements:	SI-04(17).01-00	(17) The organization correlates results from monitoring physical, cyber, and supply chain activities to achieve integrated situational awareness.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Integrated situational awareness enhances the capability of the organization to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out the attacks.	Y		
		SI-05.01-00	SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-05.01-00	Control: The organization:	Y		
		SI-05.01-01		SI-05.01-01	a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;	Y		
		SI-05.01-02		SI-05.01-02	b. Generates internal security alerts, advisories, and directives as deemed necessary;	Y		
		SI-05.01-03		SI-05.01-03	c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and	Y		
		SI-05.01-04		SI-05.01-04	d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	Y		
				Supplemental Guidance	Supplemental Guidance: Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance	Y		
		SI-05(1).01-00	Control Enhancements:	SI-05(1).01-00	(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	Y		
		SI-06.01-00	SI-6 SECURITY FUNCTIONALITY VERIFICATION	SI-06.01-00	Control: The information system verifies the correct operation of security functions [*Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]*] and [*Selection (one or more): notifies system administrator;*	Y		
				Supplemental Guidance	Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional states	Y		
		SI-06(1).01-00	Control Enhancements:	SI-06(1).01-00	(1) The information system provides notification of failed automated security tests.	Y		
		SI-06(2).01-00	Control Enhancements:	SI-06(2).01-00	(2) The information system provides automated support for the management of distributed security testing.	Y		
		SI-06(3).01-00	Control Enhancements:	SI-06(3).01-00	(3) The organization reports the result of security function verification to designated organizational officials with information security responsibilities.	Y		
				Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Organizational officials with information security responsibilities include, for example, senior information security officers, information system security managers, and information systems security officers.	Y		
		SI-07.01-00	SI-7 SOFTWARE AND INFORMATION INTEGRITY	SI-07.01-00	Control: The information system detects unauthorized changes to software and information.	Y		
				Supplemental Guidance	Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy	Y		
		SI-07(1).01-00	Control Enhancements:	SI-07(1).01-00	(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system.	Y		
		SI-07(2).01-00	Control Enhancements:	SI-07(2).01-00	(2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.	Y		
		SI-07(3).01-00	Control Enhancements:	SI-07(3).01-00	(3) The organization employs centrally managed integrity verification tools.	Y		
		SI-07(4).01-00	Control Enhancements:	SI-07(4).01-00	(4) The organization requires use of tamper-evident packaging for [*Assignment: organization-defined information system components*] during [*Selection: transportation from vendor to operational site; during operation; both*].	Y		
		SI-08.01-00	SI-8 SPAM PROTECTION	SI-08.01-00	Control: The organization:	Y		
		SI-08.01-01		SI-08.01-01	a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and	Y		
		SI-08.01-02		SI-08.01-02	b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	Y		
				Supplemental Guidance	Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.	Y		
		SI-08(1).01-00	Control Enhancements:	SI-08(1).01-00	(1) The organization centrally manages spam protection mechanisms.	Y		
		SI-08(2).01-00	Control Enhancements:	SI-08(2).01-00	(2) The information system automatically updates spam protection mechanisms (including signature definitions).	Y		
		SI-09.01-00	SI-9 INFORMATION INPUT RESTRICTIONS	SI-09.01-00	Control: The organization restricts the capability to input information to the information system to authorized personnel.	Y		
					Supplemental Guidance: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.	Y		
		SI-10.01-00	SI-10 INFORMATION INPUT VALIDATION	SI-10.01-00	Control: The information system checks the validity of information inputs.	Y		
					Supplemental Guidance: Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally	Y		
		SI-11.01-00	SI-11 ERROR HANDLING	SI-11.01-00	Control: The information system:	Y		
		SI-11.01-01		SI-11.01-01	a. Identifies potentially security-relevant error conditions;	Y		
		SI-11.01-02		SI-11.01-02	b. Generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries; and	Y		
		SI-11.01-03		SI-11.01-03	c. Reveals error messages only to authorized personnel.	Y		
				Supplemental Guidance	Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security	Y		

	SI-12.01-00	SI-12 INFORMATION OUTPUT HANDLING AND RETENTION	SI-12.01-00	Control: The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	Y		
			Supplemental Guidance	Supplemental Guidance: The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention. Related controls: MP-2, MP-4.	Y		
	SI-13.01-00	SI-13 PREDICTABLE FAILURE PREVENTION	SI-13.01-00	Control: The organization:	Y		
	SI-13.01-01		SI-13.01-01	a. Protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation; and	Y		
	SI-13.01-02		SI-13.01-02	b. Provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components.	Y		
			Supplemental Guidance	Supplemental Guidance: While mean time to failure is primarily a reliability issue, this control focuses on the potential failure of specific components of the information system that provide security capability. Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry-average. The transfer of	Y		
	SI-13(1).01-00	Control Enhancements:	SI-13(1).01-00	(1) The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.	Y		
	SI-13(2).01-00	Control Enhancements:	SI-13(2).01-00	(2) The organization does not allow a process to execute without supervision for more than [*Assignment: organization-defined time period*].	Y		
	SI-13(3).01-00	Control Enhancements:	SI-13(3).01-00	(3) The organization manually initiates a transfer between active and standby information system components at least once per [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].	Y		
	SI-13(4).01-00	Control Enhancements:	SI-13(4).01-00	(4) The organization, if an information system component failure is detected:	Y		
	SI-13(4).01-01	Control Enhancements:	SI-13(4).01-01	(a) Ensures that the standby information system component successfully and transparently assumes its role within [*Assignment: organization-defined time period*]; and	Y		
	SI-13(4).01-02	Control Enhancements:	SI-13(4).01-02	(b) [*Selection (one or more): activates* [*Assignment: organization-defined alarm*]; *automatically shuts down the information system*].	Y		
			Enhanced Supplemental Guidance	Enhancement Supplemental Guidance: Automatic or manual transfer of roles to a standby unit may occur upon detection of a component failure.	Y		
	PM-01.01-00	PM-1 INFORMATION SECURITY PROGRAM PLAN	PM-01.01-00	Control: The organization:	Y		
	PM-01.01-01		PM-01.01-01	a. Develops and disseminates an organization-wide information security program plan that:	Y		
	PM-01.01-02		PM-01.01-02	b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and	Y		
	PM-01.01-03		PM-01.01-03	c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	Y		
			Supplemental Guidance	Supplemental Guidance: The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the	Y		
			Supplemental Guidance	Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization	Y		
	PM-02.01-00	PM-2 SENIOR INFORMATION SECURITY OFFICER	PM-02.01-00	Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Y		
			Supplemental Guidance	Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this organizational official as the Senior Information	Y		
	PM-03.01-00	PM-3 INFORMATION SECURITY RESOURCES	PM-03.01-00	Control: The organization:	Y		
	PM-03.01-01		PM-03.01-01	a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;	Y		
	PM-03.01-02		PM-03.01-02	b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and	Y		
	PM-03.01-03		PM-03.01-03	c. Ensures that information security resources are available for expenditure as planned.	Y		
				Supplemental Guidance: Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.	Y		
	PM-04.01-00	PM-4 PLAN OF ACTION AND MILESTONES PROCESS	PM-04.01-00	Control: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	Y		
			Supplemental Guidance	Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB	Y		
	PM-05.01-00	PM-5 INFORMATION SYSTEM INVENTORY	PM-05.01-00	Control: The organization develops and maintains an inventory of its information systems.	Y		
			Supplemental Guidance	Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.	Y		
	PM-06.01-00	PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE	PM-06.01-00	Control: The organization develops, monitors, and reports on the results of information security measures of performance.	Y		
			Supplemental Guidance	Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.	Y		
	PM-07.01-00	PM-7 ENTERPRISE ARCHITECTURE	PM-07.01-00	Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	Y		
			Supplemental Guidance	Supplemental Guidance: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in	Y		
	PM-08.01-00	PM-8 CRITICAL INFRASTRUCTURE PLAN	PM-08.01-00	Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Y		
			Supplemental Guidance	Supplemental Guidance: The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.	Y		
	PM-09.01-00	PM-9 RISK MANAGEMENT STRATEGY	PM-09.01-00	Control: The organization:	Y		
	PM-09.01-01		PM-09.01-01	a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and	Y		
	PM-09.01-02		PM-09.01-02	b. Implements that strategy consistently across the organization.	Y		

					Supplemental Guidance	Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and	Y		
			PM-10.01-00	PM-10 SECURITY AUTHORIZATION PROCESS	PM-10.01-00	Control: The organization:	Y		
			PM-10.01-01		PM-10.01-01	a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;	Y		
			PM-10.01-02		PM-10.01-02	b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and	Y		
			PM-10.01-03		PM-10.01-03	c. Fully integrates the security authorization processes into an organization-wide risk management program.	Y		
					Supplemental Guidance	Supplemental Guidance: The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information	Y		
			PM-11.01-00	PM-11 MISSION/BUSINESS PROCESS DEFINITION	PM-11.01-00	Control: The organization:	Y		
			PM-11.01-01		PM-11.01-01	a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and	Y		
			PM-11.01-02		PM-11.01-02	b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	Y		
					Supplemental Guidance	Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
HIPAA

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence	Source
HIPAA	00	0	HIPAA.00.0	CITATIONS	GENERAL ROLES	Vendor will comply with all HIPAA GENERAL ROLES				
HIPAA	00	1	HIPAA.00.1	164.306(a)	Ensure Confidentiality, Integrity and Availability	(a) General requirements. Vendor must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	Y			
HIPAA	00	2	HIPAA.00.2	164.306(b)	Flexibility of Approach	(b) Flexibility of approach. (1) Vendor may use any security measures that allow the vendor to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a vendortake into account the following factors: (i) The size, complexity, and capabilities of the covered entity. (ii) The vendor's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures.	Y			
HIPAA	00	3	HIPAA.00.3	164.306(c)	Standards	(c) Standards. A vendor must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.	Y			
HIPAA	00	4	HIPAA.00.4	164.306(d)	Implementation Specifications	(d) Implementation specifications. In this subpart: (1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification. (2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications. (3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must-- (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and (ii) As applicable to the entity-- (A) Implement the implementation specification if reasonable and appropriate; or (B) If implementing the implementation specification is not reasonable and appropriate-- (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and	Y			
HIPAA	00	5	HIPAA.00.5	164.306(e)	Maintenance	(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.	Y			
HIPAA	01	0	HIPAA.01.0	CITATIONS	ADMINISTRATIVE SAFEGUARDS	Vendor will comply with all HIPAA ADMINISTRATIVE SAFEGUARDS				
HIPAA	01	1	HIPAA.01.1	164.308(a)(1)(i)	Security Management Process	Vendor will implement policies and procedures to prevent, detect, contain and correct security violations	Y			
HIPAA	01	2	HIPAA.01.2	164.308(a)(1)(ii)(A)	Risk Analysis	Vendor will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Y			
HIPAA	01	3	HIPAA.01.3	164.308(a)(1)(ii)(B)	Risk Management	Vendor will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec 164.306(a).	Y			
HIPAA	01	4	HIPAA.01.4	164.308(a)(1)(ii)(C)	Sanction Policy	Vendor will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	Y			
HIPAA	01	5	HIPAA.01.5	164.308(a)(1)(ii)(D)	Information System Activity Review	Vendor will implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Y			
HIPAA	01	6	HIPAA.01.6	164.308(a)(2)	Assigned Security Responsibility	Vendor will identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Y			
HIPAA	01	7	HIPAA.01.7	164.308(a)(3)(i)	Workforce Security	Vendor will implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Y			
HIPAA	01	8	HIPAA.01.8	164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Vendor will implement procedures for authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Y			
HIPAA	01	9	HIPAA.01.9	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Vendor will implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Y			
HIPAA	01	10	HIPAA.01.10	164.308(a)(3)(ii)(C)	Termination Procedures	Vendor will implement procedures for termination access to electronic protected health information when the employment of a workforce member ends or as required by determination made as specified in paragraph (a)(3)(ii)(B) of this section.	Y			
HIPAA	01	11	HIPAA.01.11	164.308(a)(4)(i)	Information Access Management	Vendor will implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Y			
HIPAA	01	12	HIPAA.01.12	164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement polices and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Y			
HIPAA	01	13	HIPAA.01.13	164.308(a)(4)(ii)(B)	Access Authorization	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process or other mechanism.	Y			
HIPAA	01	14	HIPAA.01.14	164.308(a)(4)(ii)(C)	Access Establishment and Modification	Vendor will implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Y			
HIPAA	01	15	HIPAA.01.15	164.308(a)(5)(i)	Security Awareness Training	Vendor will implement a security awareness and training program for all members of its workforce (including management).	Y			
HIPAA	01	16	HIPAA.01.16	164.308(a)(5)(ii)(A)	Security Reminders	Vendor will distribute periodic security updates.	Y			
HIPAA	01	17	HIPAA.01.17	164.308(a)(5)(ii)(B)	Protection from Malicious Software	Vendor will have procedures for guarding against, detecting, and reporting malicious software.	Y			
HIPAA	01	18	HIPAA.01.18	164.308(a)(5)(ii)(C)	Log-in Monitoring	Vendor will have procedures for monitoring log-in attempts and reporting discrepancies.	Y			
HIPAA	01	19	HIPAA.01.19	164.308(a)(5)(ii)(D)	Password Management	Vendor will have procedures for creating, changing, and safeguarding passwords.	Y			
HIPAA	01	20	HIPAA.01.20	164.308(a)(6)(i)	Security Incident Procedures	Vendor will implement policies and procedures to address security incidents.	Y			
HIPAA	01	21	HIPAA.01.21	164.308(a)(6)(ii)	Response and Reporting	Vendor will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Y			
HIPAA	01	22	HIPAA.01.22	164.308(a)(7)(i)	Contingency Plan	Vendor will establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Y			
HIPAA	01	23	HIPAA.01.23	164.308(a)(7)(ii)(A)	Data Backup Plan	Vendor will establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Y			
HIPAA	01	24	HIPAA.01.24	164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Vendor will establish (and implement as needed) procedures to restore loss of data.	Y			
HIPAA	01	25	HIPAA.01.25	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Vendor will establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operation in emergency mode.	Y			
HIPAA	01	26	HIPAA.01.26	164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Vendor will implement procedures for periodic testing and revision of contingency plans.	Y			
HIPAA	01	27	HIPAA.01.27	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Vendor will assess the relative criticality of specific applications and data in support of other contingency plan components.	Y			
HIPAA	01	28	HIPAA.01.28	164.308(a)(8)	Evaluation	Vendor will perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Y			
HIPAA	01	29	HIPAA.01.29	164.308(b)(1)	Business Associate Contracts and Other Arrangements	Covered Entity, in accordance with § 164.306, may permit a business associate (Vendor) to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.	Y			
HIPAA	01	30	HIPAA.01.30	164.308(b)(4)	Written Contract	Vendor will sign document (contract) the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	Y			
HIPAA	02	0	HIPAA.02.0	CITATIONS	PHYSICAL SAFEGUARDS	Vendor will comply with all HIPAA PHYSICAL SAFEGUARDS				

HIPAA	02	1	HIPAA.02.1	164.310(a)(1)	Facility Access Controls	Vendor will implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Y			
HIPAA	02	2	HIPAA.02.2	164.310(a)(2)(i)	Contingency Operations	Vendor will establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Y			
HIPAA	02	3	HIPAA.02.3	164.310(a)(2)(ii)	Facility Security Plan	Vendor will implement policies and procedures to safeguard the facility and the equipment there in from unauthorized physical access, tampering, and theft.	Y			
HIPAA	02	4	HIPAA.02.4	164.310(a)(2)(iii)	Access Control Validation Procedures	Vendor will implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Y			
HIPAA	02	5	HIPAA.02.5	164.310(a)(2)(iv)	Maintenance Records	Vendor will implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).	Y			
HIPAA	02	6	HIPAA.02.6	164.310(b)	Workstation Use	Vendor will implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Y			
HIPAA	02	7	HIPAA.02.7	164.310(c)	Workstation Security	Vendor will implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Y			
HIPAA	02	8	HIPAA.02.8	164.310(d)(1)	Device and Media Controls	Vendor will implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Y			
HIPAA	02	9	HIPAA.02.9	164.310(d)(2)(i)	Disposal	Vendor will implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Y			
HIPAA	02	10	HIPAA.02.10	164.310(d)(2)(ii)	Media Re-use	Vendor will implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	Y			
HIPAA	02	11	HIPAA.02.11	164.310(d)(2)(iii)	Accountability	Vendor will maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Y			
HIPAA	02	12	HIPAA.02.12	164.310(d)(2)(iv)	Data Backup and Storage	Vendor will create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Y			
HIPAA	03	0	HIPAA.03.0	CITATIONS	TECHNICAL SAFEGUARDS	Vendor will comply with all HIPAA TECHNICAL SAFEGUARDS				
HIPAA	03	1	HIPAA.03.1	164.312(a)(1)	Access Control	Vendor will implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Y			
HIPAA	03	2	HIPAA.03.2	164.312(a)(2)(i)	Unique User Identification	Vendor will assign a unique name and/or number for identifying and tracking user identity.	Y			
HIPAA	03	3	HIPAA.03.3	164.312(a)(2)(ii)	Emergency Access Procedure	Vendor will establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Y			
HIPAA	03	4	HIPAA.03.4	164.312(a)(2)(iii)	Automatic Logoff	Vendor will implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Y			
HIPAA	03	5	HIPAA.03.5	164.312(a)(2)(iv)	Encryption and Decryption	Vendor will implement a mechanism to encrypt and decrypt electronic protected health information.	Y			
HIPAA	03	6	HIPAA.03.6	164.312(b)	Audit Controls	Vendor will implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Y			
HIPAA	03	7	HIPAA.03.7	164.312(c)(1)	Integrity	Vendor will implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Y			
HIPAA	03	8	HIPAA.03.8	164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	Vendor will implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Y (limited)			
HIPAA	03	9	HIPAA.03.9	164.312(d)	Person or Entity Authentication	Vendor will implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Y			
HIPAA	03	10	HIPAA.03.10	164.312(e)(1)	Transmission Security	Vendor will implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Y			
HIPAA	03	11	HIPAA.03.11	164.312(e)(2)(i)	Integrity Controls	Vendor will implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Y			
HIPAA	03	12	HIPAA.03.12	164.312(e)(2)(ii)	Encryption	Vendor will implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Y			
HIPAA	04	0	HIPAA.04.0	CITATIONS	ORGANIZATIONAL REQUIREMENTS					
HIPAA	04	1	HIPAA.04.1	164.314(a)(1)	Business Associate Contracts or Other Arrangements	(i) The contract or other arrangement between the covered entity and its business associate (Vendor) required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful. (A) Terminated the contract or arrangement, if feasible; or	Y			
HIPAA	04	2	HIPAA.04.2	164.314(a)(2)	Business Associate Contracts	(i) Business associate contracts. The contract between a covered entity and a business associate (Vendor) must provide that the business associate will-- (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. (ii) Other arrangements. (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if - (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section. (B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. (C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as	Y			
HIPAA	04	3	HIPAA.04.3	164.314(b)(1)	Requirements for Group Health Plans	Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Y (limited)	Limited to the Plan electronic data exchanges		
HIPAA	04	4	HIPAA.04.4	164.314(b)(2)(i)	Implement Safeguards	The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;	Y (limited)	Limited to the Plan electronic data exchanges		
HIPAA	04	5	HIPAA.04.5	164.314(b)(2)(ii)	Ensure Adequate Separation	Vendor will ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;	Y			
HIPAA	04	6	HIPAA.04.6	164.314(b)(2)(iii)	Ensure Agents Safeguard	Vendor will ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and	Y			
HIPAA	04	7	HIPAA.04.7	164.314(b)(2)(iv)	Report Security Incidents	Vendor will report to the group health plan any security incident of which it becomes aware.	Y			
HIPAA	04	8	HIPAA.04.8	164.316(a)	Policies and Procedures	A covered entity must, in accordance with § 164.306: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	Y			

HIPAA	04	9	HIPAA.04.9	164.316(b)(1)	Documentation	Documentation. (i) Vendor will maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Y			
HIPAA	04	10	HIPAA.04.10	164.316(b)(2)(i)	Time Limit	Vendor will retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Y			
HIPAA	04	11	HIPAA.04.11	164.316(b)(2)(ii)	Availability	Vendor will make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Y			
HIPAA	04	12	HIPAA.04.12	164.316(b)(2)(iii)	Updates	Vendor will reviews documentation periodically, and updates as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Y			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
PHI and Privacy

Base	Level	Seq	Req ID Note	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence	Source
PHI	01	0	PHI.01.0	PHI and Privacy,		If Customer is subject to the Health Insurance Portability and Accountability Act (HIPAA), beginning in February 2010, Customer is required to ensure that service providers take specific measures to help safeguard Customer's electronic PHI (ePHI) that they may store or access. These measures are specified in Section 13400 et seq. of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, which act amends HIPAA.	Y			
PHI	01	1	PHI.01.1	PHI and Privacy,	Testing and Revision Procedures	Hosting Provider shall implement procedures for periodic testing and revision of contingency plans.	Y			
PHI	01	2	PHI.01.2	PHI and Privacy,	Encryption	Hosting Provider shall implement a mechanism to encrypt ePHI whenever deemed appropriate.	Y			
PHI	01	3	PHI.01.3	PHI and Privacy,		Except when the only electronic PHI disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic PHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Y			
PHI	01	4	PHI.01.4	PHI and Privacy, Access Control (§ 164.312(a)(1))	Data Backup and Storage	Hosting Provider shall create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Y			
PHI	01	5	PHI.01.5	PHI and Privacy, Access Control (§ 164.312(a)(1))		Covered entities must implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted appropriate access rights.	Y			
PHI	01	6	PHI.01.6	PHI and Privacy, Access Control (§ 164.312(a)(1))	Unique User Identification	Hosting Provider shall assign a unique name and/or number for identifying and tracking user identity.	Y			
PHI	01	7	PHI.01.7	PHI and Privacy, Access Control (§ 164.312(a)(1))	Emergency Access Procedure	Hosting Provider shall establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.	Y			
PHI	01	8	PHI.01.8	PHI and Privacy, Access Control (§ 164.312(a)(1))	Automatic Logoff	Hosting Provider implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Y			
PHI	01	9	PHI.01.9	PHI and Privacy, Assigned Security Responsibility (§ 164.308(a)(2))	Information System Activity Review	Hosting Provider shall implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. (§164.308(a)(1)(ii)(D))	Y			
PHI	01	10	PHI.01.10	PHI and Privacy, Audit Controls (§ 164.312(b))	Encryption and Decryption	Hosting Provider shall implement a mechanism to encrypt and decrypt ePHI.	Y			
PHI	01	11	PHI.01.11	PHI and Privacy, Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))		Hosting Provider shall engage a third party auditor to assess Hosting Provider and HIPAA Security Services for compliance with the HIPAA Privacy and Security Rule. The audit report will be available annually to Customer.	Y			
PHI	01	12	PHI.01.12	PHI and Privacy, Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))		Covered entities must -- when dealing with business associates that create, receive, maintain, or transmit ePHI on the covered entities behalf -- develop and implement contracts that ensure the business associate will appropriately safeguard the information.	Y			
PHI	01	13	PHI.01.13	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))	Business Associate Contracts	Hosting Provider shall create a contract with the covered entity and the business associate must prove that the business associate will:	Y			
PHI	01	14	PHI.01.14	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))		Hosting Provider shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart. (§ 164.314 (a)(2)(i)(A)).	Y			
PHI	01	15	PHI.01.15	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))		Hosting Provider shall Ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it. (§ 164.314 (a)(2)(i)(B)).	Y			
PHI	01	16	PHI.01.16	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))		Hosting Provider shall Report to the covered entity any security incident of which it becomes aware. (§ 164.314 (a)(2)(i)(C)).	Y			
PHI	01	17	PHI.01.17	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Response and Reporting	Hosting Provider shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Y			
PHI	01	18	PHI.01.18	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))		Covered entities must establish and implement as needed policies and procedures for responding to a disaster or emergency that damages information systems containing ePHI.	Y			
PHI	01	19	PHI.01.19	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Data Backup Plan	Hosting Provider shall establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Y			
PHI	01	20	PHI.01.20	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Disaster Recovery Plan	Hosting Provider shall establish (and implement as needed) procedures to restore any loss of data.	Y			
PHI	01	21	PHI.01.21	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Emergency Model Operation Plan	Hosting Provider shall establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	Y			
PHI	01	22	PHI.01.22	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))		Covered entities must implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. (Required)	Y			
PHI	01	23	PHI.01.23	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))		Covered entities must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.	Y			
PHI	01	24	PHI.01.24	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))	Disposal	Hosting Provider shall implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Y			
PHI	01	25	PHI.01.25	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))	Media Reuse	Hosting Provider shall implement procedures for removal of ePHI from electronic media before the media are made available for re-use.	Y			
PHI	01	26	PHI.01.26	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))	Accountability	Hosting Provider shall maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Y			
PHI	01	27	PHI.01.27	PHI and Privacy, Evaluation (§ 164.308(a)(8))	Application and Data Criticality	Hosting Provider shall assess the relative criticality of specific applications and data in support of other Contingency Plan components.	Y			
PHI	01	28	PHI.01.28	PHI and Privacy, Evaluation (§ 164.308(a)(8))		Covered Entities must perform periodic technical and non-technical evaluations that determine the extent to which their security policies, procedures, and processes meet the ongoing requirements of the Security Rule and the evolving standards for the protection of ePHI. (Required)	Y			
PHI	01	29	PHI.01.29	PHI and Privacy, Evaluation (§ 164.308(a)(8))		Hosting Providers must plan to employ an external auditor to regularly perform SSAE No. 16/ ISAE No. 3402 audits on its Computer and Administration Services to assess the soundness of security policies, procedures and controls	Y			
PHI	01	30	PHI.01.30	PHI and Privacy, Evaluation (§ 164.308(a)(8))	ISO 27002 Certificate of Conformance -	Hosting Provider must have received the ISO 27002 Certificate of Conformance.	Y			
PHI	01	31	PHI.01.31	PHI and Privacy, Evaluation (§ 164.308(a)(8))	ISO 27001 Certification	Hosting Provider shall possess ISO 27001 certification. The scope of this certification encompasses the staff, technology and processes in the Hosting Provider Security Services team.	Y			

PHI	01	32	PHI.01.32	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Written Contracts or other Arrangements	A covered entity, in accordance with § 164.306 (General Rules), may permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.	Y			
PHI	01	33	PHI.01.33	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))		Covered entities must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Y			
PHI	01	34	PHI.01.34	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))		Hosting providers shall establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.	Y			
PHI	01	35	PHI.01.35	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Facility Security Plan	Customer and hosting provider(s) shall implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Y			
PHI	01	36	PHI.01.36	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Access Control and Validation Procedures	Hosting Provider shall implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Y			
PHI	01	37	PHI.01.37	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Maintenance Records	Hosting Provider shall implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors and locks).	Y			
PHI	01	38	PHI.01.38	PHI and Privacy, General Scope of Services		Hosting Provider will procure "Secure Site Pro with Extended Validation" SSL certificates from the Third Party Vendor Verisign and configure Internet facing URLs on the Hosting Provider ePHI Environments to make use of such certificates. Secure Site Pro with Extended Validation SSL certificates are designed to provide a greater level of protection against phishing and man-in-the middle attacks than the standard Secure Site Pro SSL certificates, and are intended to enforce strong encryption of user traffic between a client browser and a hosted environment	Y			
PHI	01	39	PHI.01.39	PHI and Privacy, Information Access Management (§ 164.308(a)(4))	Termination Procedures	Hosting Provider shall implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made as specified in the workforce clearance procedure paragraph.	Y			
PHI	01	40	PHI.01.40	PHI and Privacy, Information Access Management (§ 164.308(a)(4))		The covered entity must implement policies, procedures, and processes for authorizing, establishing, and modifying access to ePHI.	Y			
PHI	01	41	PHI.01.41	PHI and Privacy, Information Access Management (§ 164.308(a)(4))	Isolating Health Care Clearinghouse Functions	Hosting Provider shall: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	Y			
PHI	01	42	PHI.01.42	PHI and Privacy, Information Access Management (§ 164.308(a)(4))	Access Authorization	Hosting Provider shall implement policies and procedures for granting access to ePHI	Y			
PHI	01	43	PHI.01.43	PHI and Privacy, Integrity (§ 164.312(c)(1))		Covered entities must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. (Required)	Y			
PHI	01	44	PHI.01.44	PHI and Privacy, Notification in the Case of Breach of Unsecured PHI (§ 164.410)	ePHI Documentation Review	Hosting Provider shall review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic PHI.	Y			
PHI	01	45	PHI.01.45	PHI and Privacy, Notification in the Case of Breach of Unsecured PHI (§ 164.410)		A business associate shall, following the discovery of a breach of unsecured PHI, notify the covered entity of such breach.	Y			
PHI	01	46	PHI.01.46	PHI and Privacy, Notification in the Case of Breach of Unsecured PHI (§ 164.410)	Timeliness of Notification	Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of the section without unreasonable delay and in no case later than 30 calendar days after discovery of a breach.	Y			
PHI	01	47	PHI.01.47	PHI and Privacy, Person or Entity Authentication (§ 164.312(d))		Covered entities must implement policies and procedures to protect electronic PHI from improper alteration or destruction.	Y			
PHI	01	48	PHI.01.48	PHI and Privacy, Person or Entity Authentication (§ 164.312(d))	Mechanism to Authenticate ePHI	Hosting Provider shall implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Y			
PHI	01	49	PHI.01.49	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Policies and Procedures	Hosting Provider shall: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart. This standard is not to be construed to permit or excuse an action that violates any	Y			
PHI	01	50	PHI.01.50	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Documentation	Hosting Provider shall: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. (§ 164.316(b)(1)).	Y			
PHI	01	51	PHI.01.51	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Time Limit	Hosting Provider shall retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Y			
PHI	01	52	PHI.01.52	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Documentation Availability	Hosting Provider shall make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Y			
PHI	01	53	PHI.01.53	PHI and Privacy, Privacy Requirements		In order to help Customer meet these new security related obligations under HITECH, Hosting Provider Hosting Provider has developed the HIPAA Security Services. This offering employs additional security controls that supplement the standard Hosting Provider security practices and are aligned with the standards established by HITECH.	Y			
PHI	01	54	PHI.01.54	PHI and Privacy, Requirements for Group Health Plans (§ 164.314(b)(1))		Hosting Provider shall Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. (§ 164.314 (a)(2)(i)(D)).	Y			
PHI	01	55	PHI.01.55	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))		Access Establishment and Modification (Addressable): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Y			
PHI	01	56	PHI.01.56	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))		Covered entities must implement a security awareness and training program for all members of its workforce (including management).	Y			
PHI	01	57	PHI.01.57	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))	Security Reminders	Hosting Provider shall implement periodic security updates.	Y			
PHI	01	58	PHI.01.58	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))	Protection From Malicious Software	Hosting Provider shall procedures for guarding against, detecting, and reporting malicious software.	Y			

PHI	01	59	PHI.01.59	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))	Login Monitoring	Hosting Provider shall create procedures for monitoring log-in attempts and reporting discrepancies.	Y			
PHI	01	60	PHI.01.60	PHI and Privacy, Security Incident Procedures (§ 164.308(a)(6))	Password Management	Hosting Provider shall create procedures for creating, changing, and safeguarding passwords.	Y			
PHI	01	61	PHI.01.61	PHI and Privacy, Security Incident Procedures (§ 164.308(a)(6))		The covered entity must implement policies, procedures, and processes for reporting, responding to, and managing security incidents.	Y			
PHI	01	62	PHI.01.62	PHI and Privacy, Security Management Process (§ 164.308(a)(1))		Hosting Provider shall address the HIPAA security obligations for business associates with respect to ePHI to the extent they are applicable to the Computer and Administration Services.	Y			
PHI	01	63	PHI.01.63	PHI and Privacy, Security Management Process (§ 164.308(a)(1))		Covered entities must implement policies and procedures to prevent, detect, contain, and correct security violations.	Y			
PHI	01	64	PHI.01.64	PHI and Privacy, Security Management Process (§ 164.308(a)(1))	Risk Analysis	Customer or its hosting provider(s) shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity. (§164.308(a)(1)(ii)(A)).	Y			
PHI	01	65	PHI.01.65	PHI and Privacy, Security Management Process (§ 164.308(a)(1))	Risk Management	Hosting Provider shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a). (§164.308(a)(1)(ii)(B))	Y			
PHI	01	66	PHI.01.66	PHI and Privacy, Security Management Process (§ 164.308(a)(1))	Sanction Policy	Hosting Provider shall develop policies and procedures for imposing appropriate sanctions (e.g., reprimand, termination) for noncompliance with the organization's security policies. (§164.308(a)(1)(ii)(C))	Y			
PHI	01	67	PHI.01.67	PHI and Privacy, Security Requirements		Hosting Provider shall authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. (§ 164.504 (e)(2)(iii))	Y			
PHI	01	68	PHI.01.68	PHI and Privacy, Transmission Security (§ 164.312(e)(1))		Covered entities must implement procedures to verify that a person or entity seeking access to ePHI is who or what they claim to be. (Required)	Y			
PHI	01	69	PHI.01.69	PHI and Privacy, Transmission Security (§ 164.312(e)(1))		Covered entities must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	Y			
PHI	01	70	PHI.01.70	PHI and Privacy, Transmission Security (§ 164.312(e)(1))	Integrity Controls	Hosting Provider shall implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Y			
PHI	01	71	PHI.01.71	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		The following practices describe how Hosting Provider has addressed the HIPAA privacy obligations for business associates with respect to PHI set forth in 45 C.F.R. 164.504(e)(2) to the extent they are applicable to Computer and Administration Services.	Y			
PHI	01	72	PHI.01.72	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Customer and hosting provider(s) shall establish the permitted and required uses and disclosures of such information by the business associate. (§ 164.504 (e)(2)(i))	Y			
PHI	01	73	PHI.01.73	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Customer and hosting provider(s) shall not use or further disclose the information other than as permitted or required by the contract or as required by law. (§ 164.504 (e)(2)(ii)(A))	Y			
PHI	01	74	PHI.01.74	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Customer and hosting provider(s) shall use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract. (§ 164.504 (e)(2)(ii)(B))	Y			
PHI	01	75	PHI.01.75	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Hosting Provider shall report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware. (§ 164.504 (e)(2)(ii)(C))	Y			
PHI	01	76	PHI.01.76	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Hosting Provider shall ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information. (§ 164.504 (e)(2)(ii)(D))	Y			
PHI	01	77	PHI.01.77	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Hosting Provider shall make available PHI in accordance with §164.524. (§ 164.504 (e)(2)(ii)(E))	Y			
PHI	01	78	PHI.01.78	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Hosting Provider shall make available PHI for amendment and incorporate any amendments to PHI in accordance with §164.526. (§ 164.504 (e)(2)(ii)(F))	Y			
PHI	01	79	PHI.01.79	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Hosting Provider shall make available the information required to provide an accounting of disclosures in accordance with §164.528. (§ 164.504 (e)(2)(ii)(G))	Y			
PHI	01	80	PHI.01.80	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Hosting Provider shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart. (§ 164.504 (e)(2)(ii)(H))	Y			
PHI	01	81	PHI.01.81	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		Hosting Provider shall, at termination of any contracts, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. (§ 164.504 (e)(2)(ii)(I))	Y			
PHI	01	82	PHI.01.82	PHI and Privacy, Workforce Security (§ 164.308(a)(3))		A covered entity must identify a security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. (Required)	Y			
PHI	01	83	PHI.01.83	PHI and Privacy, Workforce Security (§ 164.308(a)(3))		A covered entity must implement policies, procedures and processes to ensure that all members of its workforce have appropriate access to ePHI and workforce members without access are not able to obtain it.	Y			
PHI	01	84	PHI.01.84	PHI and Privacy, Workforce Security (§ 164.308(a)(3))	Authorization and or Supervision	Hosting Provider shall implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. (§ 164.308(a)(3)(ii)(A))	Y			
PHI	01	85	PHI.01.85	PHI and Privacy, Workforce Security (§ 164.308(a)(3))	Workforce Clearance Procedures	Hosting Provider shall implement procedures to determine that the access of a workforce member to ePHI is appropriate.	Y			
PHI	01	86	PHI.01.86	PHI and Privacy, Workstation Security (§ 164.310(c))		Covered entities must implement policies and procedures that specify appropriate use of workstations and the characteristics of the physical environment of workstations that can access ePHI. (Required)	Y			
PHI	01	87	PHI.01.87	PHI and Privacy, Workstation Use (§ 164.310(b))		Repairs and modifications to physical components related to security are documented in a physical access control application.	Y			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
IRS 1075

Base	Level	Sub	Req ID New	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence	Source
IRS	01	0	IRS.01.0	IRS 1075	Audit	The audit trail shall capture all successful login and logoff attempts.	Y			
IRS	01	1	IRS.01.1	IRS 1075	Audit	The audit trail shall be protected from unauthorized access, use, deletion or modification.	Y			
IRS	01	2	IRS.01.2	IRS 1075	Audit	The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.	Y			
IRS	01	3	IRS.01.3	IRS 1075	Audit	The audit trail shall capture all actions, connections and requests performed by privileged functions.	Y			
IRS	01	4	IRS.01.4	IRS 1075	Audit	The audit trail shall capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users).	Y			
IRS	01	5	IRS.01.5	IRS 1075	Audit	The audit trail shall capture all changes to logical access control authorities (e.g., rights, permissions).	Y			
IRS	01	6	IRS.01.6	IRS 1075	Audit	The audit trail shall capture all identification and authentication attempts.	Y			
IRS	01	7	IRS.01.7	IRS 1075	Audit	The audit trail shall capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.	Y			
IRS	01	8	IRS.01.8	IRS 1075	Audit	The audit trail shall capture all unsuccessful login and authorization attempts.	Y			
IRS	01	9	IRS.01.9	IRS 1075	Audit	The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, database).	Y			
IRS	01	10	IRS.01.10	IRS 1075	Audit	The audit trail shall capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s).	Y			
IRS	01	11	IRS.01.11	IRS 1075	Audit	The audit trail shall capture system startup and shutdown functions.	Y			
IRS	01	12	IRS.01.12	IRS 1075	Audit	The audit trail shall capture the creation, modification and deletion of objects including files, directories and user accounts.	Y			
IRS	01	13	IRS.01.13	IRS 1075	Audit	The audit trail shall capture the creation, modification and deletion of user account and group account privileges.	Y			
IRS	01	14	IRS.01.14	IRS 1075	Audit	The audit trail shall capture the creation, modification and deletion of user accounts and group accounts.	Y			
IRS	01	15	IRS.01.15	IRS 1075	Audit	The audit trail shall capture the enabling or disabling of audit report generation services.	Y			
IRS	01	16	IRS.01.16	IRS 1075	Audit	The audit trail shall capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event.	Y			
IRS	01	17	IRS.01.17	IRS 1075	Password	Passwords shall be a minimum length of 8 characters in a combination of alpha and numeric or special characters.	Y			
IRS	01	18	IRS.01.18	IRS 1075	Password	Users shall commit passwords to memory, avoid writing passwords down and never disclose passwords to others (e.g., with a co-worker in order to share files)	Y			
IRS	01	19	IRS.01.19	IRS 1075	Password	Users shall be prohibited from using their last six passwords to deter reuse of the same password.	Y			
IRS	01	20	IRS.01.20	IRS 1075	Password	Users shall be prohibited from changing their passwords for at least 15 days after a recent change. Meaning, the minimum password age limit shall be 15 days after a recent password change.	Y			
IRS	01	21	IRS.01.21	IRS 1075	Password	User account lockout feature shall disable the user account after 3 unsuccessful login attempts.	Y			
IRS	01	22	IRS.01.22	IRS 1075	Password	Use of dictionary words, popular phrases, or obvious combinations of letters and numbers in passwords shall be prohibited when possible. Obvious combinations of letters and numbers include first names, last names, initials, pet names, user accounts spelled backwards, repeating characters, consecutive numbers, consecutive letters, and other predictable combinations and permutations.	Y			
IRS	01	23	IRS.01.23	IRS 1075	Password	The information system shall routinely prompt users to change their passwords within 5-14 days before such password expires.	Y			
IRS	01	24	IRS.01.24	IRS 1075	Password	System initialization (boot) settings shall be password-protected.	Y			
IRS	01	25	IRS.01.25	IRS 1075	Password	Privileged users shall be able to override the minimum password age limit for users when necessary to perform required job functions.	Y			
IRS	01	26	IRS.01.26	IRS 1075	Password	Passwords shall not be automated through function keys, scripts or other methods where passwords may be stored on the system.	Y			
IRS	01	27	IRS.01.27	IRS 1075	Password	Passwords shall be systematically disabled after 90 days of inactivity to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods.	Y			
IRS	01	28	IRS.01.28	IRS 1075	Password	Passwords shall be changed every 90 days, at a minimum, for standard user accounts to reduce the risk of compromise through guessing, password cracking or other attack & penetration methods.	Y			
IRS	01	29	IRS.01.29	IRS 1075	Password	Passwords shall be changed every 60 days, at a minimum, for privileged user accounts to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods.	Y			
IRS	01	30	IRS.01.30	IRS 1075	Password	Password changes for standard and privileged users shall be systematically enforced where possible.	Y			
IRS	01	31	IRS.01.31	IRS 1075	Password	Null passwords shall be prohibited to reduce the risk of compromise through rogue enticement techniques or other attack and penetration methods.	Y			
IRS	01	32	IRS.01.32	IRS 1075	Password	Default vendor passwords shall be changed upon successful installation of the information system product.	Y			
IRS	01	33	IRS.01.33	IRS 1075	Password	Clear-text representation of passwords shall be suppressed (blotted out) when entered at the login screen.	Y			
IRS	01	34	IRS.01.34	IRS 1075	Password	Account lockout duration shall be permanent until an authorized system administrator reinstates the user account.	Y			
IRS	01	35	IRS.01.35	IRS 1075	General	The IRS Safeguards Report shall be correctly completed and requirements addressed if required	Y			
IRS	01	37	IRS.01.37	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment Technical Requirements	The system architecture is configured as a three-tier architecture with physically separate systems that provide layered security of the FTI and access to the database through the application is limited.	Y			
IRS	01	38	IRS.01.38	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment Technical Requirements	Each system within the architecture that receives, processes, stores or transmits FTI to an external customer through the web portal is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing.	Y			
IRS	01	39	IRS.01.39	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment Technical Requirements	Access to FTI via the web portal requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include: a unique username, PIN number, password or passphrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.	Y			
IRS	01	40	IRS.01.40	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment Technical Requirements	Each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the web portal is hardened in accordance with IRS Publication 1075 policy. The Publication 1075 policy can be met by utilizing the Safeguards Computer Security Evaluation Matrix (SCSEM) to configure the security settings for the applicable operating system of the web server, application server and database server. These SCSEMs are available for download from the IRS Safeguards web site.	Y			
IRS	01	41	IRS.01.41	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment Technical Requirements	Prior to implementing the web portal, the agency must conduct a thorough penetration test of the web portal environment to ensure the FTI is not vulnerable to internal and external threats. The results of the penetration test should be shared with the IRS Office of Safeguards, along with a corrective action plan for addressing vulnerabilities identified.	Y			

IRS	01	42	IRS.01.42	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	Additionally, when FTI is provided to customers through a web portal, the required frequency with which agencies conduct vulnerability scanning of the web portal architecture is increased to monthly to allow for more proactive vulnerability management of systems that provide FTI over the Internet.	Y			
IRS	01	43	IRS.01.43	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	In addition there are other resources available specific to web servers and web sessions to supplement the IRS Safeguards SCSEMs and ensure the FTI is secured properly in the web portal environment: •NIST Special Publication 800-44, Guidelines on Securing Public Web Servers provides guidance for deploying, configuring and managing secure web servers. •Defense Information Systems Agency (DISA) publication, Web Server Security Technical Implementation Guide, provides guidance on the technologies used to ensure the appropriate level of protection for web server connections, e.g., Secure Sockets Layer/Transport Layer Security (SSL/TLS).	Y			
IRS	01	44	IRS.01.44	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	If external customers have the ability to access FTI through the web portal, a strong authentication mechanism must be used to authenticate those external customers to the system. The authentication must use at least two pieces of information to verify the identity, one of which must be a shared secret only known to the parties involved, and issued by the agency directly to the customer. Examples of shared secrets include: a unique username, PIN number, password or passphrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely on all case documents the customer receives and does not provide assurance that it's only known to the parties involved in the communication.	Y			
IRS	01	45	IRS.01.45	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	Two factor authentication is applicable to employees and contractors, including system and application administrators with access to FTI through a web portal from a network external to the agency's network. This does not apply to the agency's customers who access FTI through a customer service web portal. All agency employees and contractors accessing FTI data remotely from an external network through an Internet web portal are required to be authenticated by an application that utilizes a two-factor authentication mechanism. Two-factor authentication (strong authentication) is defined as using at least two out of the three authentication factors: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Using strong authentication provides more protection for FTI than a simple username and password can provide.	Y			
IRS	01	46	IRS.01.46	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	Data Isolation. Software, data, and services that receive, transmit, process, or store FTI must be isolated within the cloud environment so that tenants sharing physical space cannot access their neighbors' physically co-located data and applications.	Y			
IRS	01	47	IRS.01.47	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	Service Level Agreements (SLA). The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or Service Level Agreement (SLA) with their third party cloud provider.	Y			
IRS	01	48	IRS.01.48	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	Data Encryption in Transit. FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA.	Y			
IRS	01	49	IRS.01.49	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	Data Encryption at Rest. FTI must be encrypted while at rest in the cloud. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA.	Y			
IRS	01	50	IRS.01.50	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	Security Control Validation. Agencies must validate security control implementation claims made by cloud providers through a security plan and security control assessments.	Y			
IRS	01	52	IRS.01.52	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	When FTI is stored in a shared location, the agency must have policies in place to restrict access to FTI to authorized users.	Y			
IRS	01	53	IRS.01.53	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	Programs that control the hypervisor should be secured and restricted to authorized administrators only.	Y			
IRS	01	54	IRS.01.54	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods, provided by either the virtualization solution or third party-solution, such as a virtual private network (VPN) that encapsulates the management traffic.	Y			
IRS	01	55	IRS.01.55	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	Separation between virtual machines (VMs) must be enforced, and functions which allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled.	Y			
IRS	01	56	IRS.01.56	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	Virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment. This includes being able to monitor the movement of FTI into and out of the virtual environment.	Y			
IRS	01	57	IRS.01.57	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	The VMs and hypervisor/ host OS software for each system within the virtual environment that receives, processes, stores or transmits FTI must be hardened in accordance with the requirements of Publication 1075 and be subject to frequent vulnerability testing.	Y			
IRS	01	58	IRS.01.58	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	Special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment between the hypervisor and VM should be disabled.	Y			

IRS	01	59	IRS.01.59	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	Virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur.	Y			
IRS	01	60	IRS.01.60	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	Vulnerability assessment must be performed on systems in a virtualized environment prior to system implementation.	Y			
IRS	01	61	IRS.01.61	IRS 1075	Section 9.18.12 Protecting FTI in Virtual Environments - Technical Requirements	Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need to know.	Y			
IRS	01	63	IRS.01.63	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	VoIP traffic that contains FTI should be segmented off from non-VoIP traffic via a virtual Local Area Network (vLAN) or other segmentation method. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied which restrict access to VoIP traffic which contains FTI.	Y			
IRS	01	64	IRS.01.64	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	When FTI is in-transit across the network (either Internet or state agency's network) the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode.	Y			
IRS	01	65	IRS.01.65	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in IRS Publication 1075, section 4.0, Secure Storage.	Y			
IRS	01	66	IRS.01.66	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing.	Y			
IRS	01	67	IRS.01.67	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	VoIP-ready firewalls must be used to filter VoIP traffic on the network.	Y			
IRS	01	68	IRS.01.68	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter.	Y			
IRS	01	69	IRS.01.69	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	VoIP phones must be logically protected and agencies must be able to track and audit all FTI-applicable conversations and access.	Y			
IRS	01	70	IRS.01.70	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	Soft-phone systems, i.e. software on user's computer to implement VoIP, should not be used with VoIP networks that transmit FTI.	Y			
IRS	01	71	IRS.01.71	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	Consider employing a variety of specific logical controls such as: authentication at each transition point, or at the device level, such as Media Access Control (MAC).	Y			
IRS	01	72	IRS.01.72	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	Use static IP addresses for the phones.	Y			
IRS	01	73	IRS.01.73	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	Employ an intrusion detection system that can identify and filter packets, allowing only traffic from a legitimate DHCP source.	Y			
IRS	01	75	IRS.01.75	IRS 1075	Contract Language	Contract Language for General or Technical Services. In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:	Y			
IRS	01	76	IRS.01.76	IRS 1075	Contract Language	All work will be performed under the supervision of the contractor or the contractor's responsible employees.	Y			
IRS	01	77	IRS.01.77	IRS 1075	Contract Language	Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited	Y			
IRS	01	78	IRS.01.78	IRS 1075	Contract Language	All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.	Y			
IRS	01	79	IRS.01.79	IRS 1075	Contract Language	No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.	Y			
IRS	01	80	IRS.01.80	IRS 1075	Contract Language	The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.	Y			
IRS	01	81	IRS.01.81	IRS 1075	Contract Language	The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.	Y			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
PCI-DSS

Source	Number	Sub	Reqmnt Number	Parent	Parent Reqmnt Number	Requirement Text	Requirement Applicable	Rationale	Validated	Test Scenario
NA	NA	NA	NA		Remove sensitive authentication data and limit data retention.	Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised. Remember—if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it	NA	NA	NA	NA
NA	NA	NA	NA		Protect the perimeter, internal, and wireless networks.	Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access most commonly used by intruders—the network and wireless access points.	NA	NA	NA	NA
NA	NA	NA	NA		Secure payment card applications.	Secure payment card applications. This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy avenues for compromising systems and obtaining access to cardholder data.	NA	NA	NA	NA
NA	NA	NA	NA		Monitor and control access to your systems.	Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.	NA	NA	NA	NA
NA	NA	NA	NA		Protect stored cardholder data.	Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.	NA	NA	NA	NA
NA	NA	NA	NA		Finalize remaining compliance efforts, and ensure all controls are in place.	Finalize remaining compliance efforts, and ensure all controls are in place. The intent of Milestone Six is to complete PCI DSS requirements and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.	NA	NA	NA	NA
PCI	1	1	PCI.1.1	PCI-DSS	6	1.1 Establish firewall and router configuration standards that include the following:	N	Note: this response applies to all entries in this section: CGI is currently not PCI compliant, CGI is currently working toward this objective to support Vermont and other State based exchanges which will include the execution of an external audit and certification		
PCI	1	1.1	PCI.1.1.1	PCI-DSS		1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.	N			
PCI	1	1.2	PCI.1.1.2	PCI-DSS	1	1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks.	N			
PCI	1	1.3	PCI.1.1.3	PCI-DSS	2	1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	N			
PCI	1	1.4	PCI.1.1.4	PCI-DSS	6	1.1.4 Description of groups, roles, and responsibilities for logical management of network components.	N			
PCI	1	1.5	PCI.1.1.5	PCI-DSS	2	1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	N			
PCI	1	1.6	PCI.1.1.6	PCI-DSS	6	1.1.6 Requirement to review firewall and router rule sets at least every six months.	N			
PCI	1	2	PCI.1.2	PCI-DSS	2	1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	N			
PCI	1	2.1	PCI.1.2.1	PCI-DSS		1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	N			
PCI	1	2.2	PCI.1.2.2	PCI-DSS	2	1.2.2 Secure and synchronize router configuration files.	N			
PCI	1	2.3	PCI.1.2.3	PCI-DSS	2	1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	N			
PCI	1	3	PCI.1.3	PCI-DSS	2	1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	N			
PCI	1	3.1	PCI.1.3.1	PCI-DSS		1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	N			
PCI	1	3.2	PCI.1.3.2	PCI-DSS	2	1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	N			
PCI	1	3.3	PCI.1.3.3	PCI-DSS	2	1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	N			
PCI	1	3.4	PCI.1.3.4	PCI-DSS	2	1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	N			
PCI	1	3.5	PCI.1.3.5	PCI-DSS	2	1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	N			
PCI	1	3.6	PCI.1.3.6	PCI-DSS	2	1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	N			
PCI	1	3.7	PCI.1.3.7	PCI-DSS	2	1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	N			
PCI	1	3.8	PCI.1.3.8	PCI-DSS	2	1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.	N			
PCI	1	4	PCI.1.4	PCI-DSS	2	1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	N			
PCI	2	0	PCI.2.0	PCI-DSS		Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	N			
PCI	2	1	PCI.2.1	PCI-DSS	2	2.1 Always change vendor-supplied defaults before installing a system on the network—including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	N			
PCI	2	1.1	PCI.2.1.1	PCI-DSS	2	2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	N			
PCI	2	2	PCI.2.2	PCI-DSS	3	2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	N			
PCI	2	2.1	PCI.2.2.1	PCI-DSS	3	2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	N			
PCI	2	2.2	PCI.2.2.2	PCI-DSS	3	2.2.2 Enable only necessary and secure services, protocols, daemons, etc. as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	N			
PCI	2	2.3	PCI.2.2.3	PCI-DSS	3	2.2.3 Configure system security parameters to prevent misuse	N			
PCI	2	2.4	PCI.2.2.4	PCI-DSS	3	2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	N			
PCI	2	3	PCI.2.3	PCI-DSS	2	2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	N			
PCI	2	4	PCI.2.4	PCI-DSS	3	2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	N			
PCI	3	0	PCI.3.0	PCI-DSS		Requirement 3: Protect stored cardholder data	N			

PCI	3	1	PCI.3.1	PCI-DSS	1	3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes as follows:	N			
PCI	3	1.1	PCI.3.1.1	PCI-DSS	1	3.1.1 Implement a data retention and disposal policy that includes: Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements. Processes for secure deletion of data when no longer needed. Specific retention requirements for cardholder data. A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	N			
PCI	3	2	PCI.3.2	PCI-DSS	1	3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3. Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.	N			
PCI	3	2.1	PCI.3.2.1	PCI-DSS	1	3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	N			
PCI	3	2.2	PCI.3.2.2	PCI-DSS	1	3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	N			
PCI	3	2.3	PCI.3.2.3	PCI-DSS	1	3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	N			
PCI	3	3	PCI.3.3	PCI-DSS	5	3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	N			
PCI	3	4	PCI.3.4	PCI-DSS	5	3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: § One-way hashes based on strong cryptography (hash must be of the entire PAN) § Truncation (hashing cannot be used to replace the truncated segment of PAN) § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key management processes and procedures Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	N			
PCI	3	4.1	PCI.3.4.1	PCI-DSS	5	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	N			
PCI	3	5	PCI.3.5	PCI-DSS	5	3.5 Protect any keys used to secure cardholder data against both disclosure and misuse: Note: This requirement also applies to key encryption keys used to protect data encrypting keys – such key encryption keys must be at least as strong as the data encrypting key.	N			
PCI	3	5.1	PCI.3.5.1	PCI-DSS	5	3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	N			
PCI	3	5.2	PCI.3.5.2	PCI-DSS	5	3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	N			
PCI	3	6	PCI.3.6	PCI-DSS	5	3.6 Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	N			
PCI	3	6.1	PCI.3.6.1	PCI-DSS	5	3.6.1 Generation of strong cryptographic keys.	N			
PCI	3	6.2	PCI.3.6.2	PCI-DSS	5	3.6.2 Secure cryptographic key distribution.	N			
PCI	3	6.3	PCI.3.6.3	PCI-DSS	5	3.6.3 Secure cryptographic key storage.	N			
PCI	3	6.4	PCI.3.6.4	PCI-DSS	5	3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	N			
PCI	3	6.5	PCI.3.6.5	PCI-DSS	5	3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	N			
PCI	3	6.6	PCI.3.6.6	PCI-DSS	5	3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	N			
PCI	3	6.7	PCI.3.6.7	PCI-DSS	5	3.6.7 Prevention of unauthorized substitution of cryptographic keys.	N			
PCI	3	6.8	PCI.3.6.8	PCI-DSS	5	3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	N			
PCI	4	0	PCI.4.0	PCI-DSS		Requirement 4: Encrypt transmission of cardholder data across open, public networks	N			
PCI	4	1	PCI.4.1	PCI-DSS	2	4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	N			
PCI	4	1.1	PCI.4.1.1	PCI-DSS	2	4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control was prohibited as of 30 June, 2010.	N			
PCI	4	2	PCI.4.2	PCI-DSS	2	4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	N			
PCI	5	0	PCI.5.0	PCI-DSS		Requirement 5: Use and regularly update anti-virus software or programs	N			
PCI	5	1	PCI.5.1	PCI-DSS	2	5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	N			
PCI	5	1.1	PCI.5.1.1	PCI-DSS	2	5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	N			
PCI	5	2	PCI.5.2	PCI-DSS	2	5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	N			
PCI	6	0	PCI.6.0	PCI-DSS		Requirement 6: Develop and maintain secure systems and applications	N			
PCI	6	1	PCI.6.1	PCI-DSS	3	6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed, install critical security patches within one month of release.	N			
PCI	6	2	PCI.6.2	PCI-DSS	3	6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Note: Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component. Note: The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.	N			
PCI	6	3	PCI.6.3	PCI-DSS	3	6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, incorporate information security throughout the software development life cycle. These processes must include the following:	N			

PCI	6	3.1	PCI.6.3.1	PCI-DSS	3	6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers.	N			
PCI	6	3.2	PCI.6.3.2	PCI-DSS	3	6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development lifecycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	N			
PCI	6	4	PCI.6.4	PCI-DSS	3	6.4 Follow change control processes and procedures for all changes to system components.	N			
PCI	6	4.1	PCI.6.4.1	PCI-DSS	3	6.4.1 Separate development/test and production environments.	N			
PCI	6	4.2	PCI.6.4.2	PCI-DSS	3	6.4.2 Separation of duties between development/test and production environments.	N			
PCI	6	4.3	PCI.6.4.3	PCI-DSS	3	6.4.3 Production data (live PANs) are not used for testing or development.	N			
PCI	6	4.4	PCI.6.4.4	PCI-DSS	3	6.4.4 Removal of test data and accounts before production systems become active.	N			
PCI	6	4.5	PCI.6.4.5	PCI-DSS	6	6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	N			
PCI	6	4.5.1	PCI.6.4.5.1	PCI-DSS	6	6.4.5.1 Documentation of impact.	N			
PCI	6	4.5.2	PCI.6.4.5.2	PCI-DSS	6	6.4.5.2 Documented change approval by authorized parties.	N			
PCI	6	4.5.3	PCI.6.4.5.3	PCI-DSS	6	6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	N			
PCI	6	4.5.4	PCI.6.4.5.4	PCI-DSS	6	6.4.5.4 Back-out procedures.	N			
PCI	6	5	PCI.6.5	PCI-DSS	3	6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: Note: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	N			
PCI	6	5.1	PCI.6.5.1	PCI-DSS	3	6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and Xpath injection flaws as well as other injection flaws.	N			
PCI	6	5.2	PCI.6.5.2	PCI-DSS	3	6.5.2 Buffer overflow.	N			
PCI	6	5.3	PCI.6.5.3	PCI-DSS	3	6.5.3 Insecure cryptographic storage.	N			
PCI	6	5.4	PCI.6.5.4	PCI-DSS	3	6.5.4 Insecure communications.	N			
PCI	6	5.5	PCI.6.5.5	PCI-DSS	3	6.5.5 Improper error handling.	N			
PCI	6	5.6	PCI.6.5.6	PCI-DSS	3	6.5.6 All "high" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). Note: This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.	N			
PCI	6	5.7	PCI.6.5.7	PCI-DSS	3	Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external): 6.5.7 Cross-site scripting (XSS).	N			
PCI	6	5.8	PCI.6.5.8	PCI-DSS	3	6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal).	N			
PCI	6	5.9	PCI.6.5.9	PCI-DSS	3	6.5.9 Cross-site request forgery (CRSF).	N			
PCI	6	6	PCI.6.6	PCI-DSS	3	6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: § Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes § Installing a web-application firewall in front of public-facing web applications	N			
PCI	7	0	PCI.7.0	PCI-DSS		Requirement 7: Restrict access to cardholder data by business need to know	N			
PCI	7	1	PCI.7.1	PCI-DSS	4	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	N			
PCI	7	1.1	PCI.7.1.1	PCI-DSS	4	Access limitations must include the following: 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	N			
PCI	7	1.2	PCI.7.1.2	PCI-DSS	4	7.1.2 Assignment of privileges is based on individual personnel's job classification and function.	N			
PCI	7	1.3	PCI.7.1.3	PCI-DSS	4	7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	N			
PCI	7	1.4	PCI.7.1.4	PCI-DSS	4	7.1.4 Implementation of an automated access control system.	N			
PCI	7	2	PCI.7.2	PCI-DSS	4	7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	N			
PCI	7	2.1	PCI.7.2.1	PCI-DSS	4	This access control system must include the following: 7.2.1 Coverage of all system components.	N			
PCI	7	2.2	PCI.7.2.2	PCI-DSS	4	7.2.2 Assignment of privileges to individuals based on job classification and function.	N			
PCI	7	2.3	PCI.7.2.3	PCI-DSS	4	7.2.3 Default "deny-all" setting.	N			
PCI	8	0	PCI.8.0	PCI-DSS		Requirement 8: Assign a unique ID to each person with computer access	N			
PCI	8	1	PCI.8.1	PCI-DSS	4	8.1 Assign all users a unique username before allowing them to access system components or cardholder data.	N			
PCI	8	2	PCI.8.2	PCI-DSS	4	8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: § Something you know, such as a password or passphrase § Something you have, such as a token device or smart card § Something you are, such as a biometric	N			
PCI	8	3	PCI.8.3	PCI-DSS	4	8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Req. 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.	N			
PCI	8	4	PCI.8.4	PCI-DSS	4	8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	N			
PCI	8	5	PCI.8.5	PCI-DSS	4	8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	N			
PCI	8	5.1	PCI.8.5.1	PCI-DSS	4	8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	N			
PCI	8	5.2	PCI.8.5.2	PCI-DSS	4	8.5.2 Verify user identity before performing password resets.	N			
PCI	8	5.3	PCI.8.5.3	PCI-DSS	4	8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	N			
PCI	8	5.4	PCI.8.5.4	PCI-DSS	4	8.5.4 Immediately revoke access for any terminated users.	N			
PCI	8	5.5	PCI.8.5.5	PCI-DSS	4	8.5.5 Remove/disable inactive user accounts at least every 90 days.	N			
PCI	8	5.6	PCI.8.5.6	PCI-DSS	4	8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	N			
PCI	8	5.7	PCI.8.5.7	PCI-DSS	4	8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	N			

PCI	8	5.8	PCI.8.5.8	PCI-DSS	4	8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	N			
PCI	8	5.9	PCI.8.5.9	PCI-DSS	4	8.5.9 Change user passwords at least every 90 days.	N			
PCI	8	5.10	PCI.8.5.10	PCI-DSS	4	8.5.10 Require a minimum password length of at least seven characters.	N			
PCI	8	5.11	PCI.8.5.11	PCI-DSS	4	8.5.11 Use passwords containing both numeric and alphabetic characters.	N			
PCI	8	5.12	PCI.8.5.12	PCI-DSS	4	8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	N			
PCI	8	5.13	PCI.8.5.13	PCI-DSS	4	8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	N			
PCI	8	5.14	PCI.8.5.14	PCI-DSS	4	8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	N			
PCI	8	5.15	PCI.8.5.15	PCI-DSS	4	8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	N			
PCI	8	5.16	PCI.8.5.16	PCI-DSS	4	8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	N			
PCI	9	0	PCI.9.0	PCI-DSS		Requirement 9: Restrict physical access to cardholder data	N			
PCI	9	1	PCI.9.1	PCI-DSS	2	9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	N			
PCI	9	1.1	PCI.9.1.1	PCI-DSS	2	9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	N			
PCI	9	1.2	PCI.9.1.2	PCI-DSS	2	9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is specifically authorized.	N			
PCI	9	1.3	PCI.9.1.3	PCI-DSS	2	9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunications lines.	N			
PCI	9	2	PCI.9.2	PCI-DSS	5	9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	N			
PCI	9	3	PCI.9.3	PCI-DSS	5	9.3 Make sure all visitors are handled as follows:	N			
PCI	9	3.1	PCI.9.3.1	PCI-DSS	5	9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	N			
PCI	9	3.2	PCI.9.3.2	PCI-DSS	5	9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	N			
PCI	9	3.3	PCI.9.3.3	PCI-DSS	5	9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	N			
PCI	9	4	PCI.9.4	PCI-DSS	5	9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	N			
PCI	9	5	PCI.9.5	PCI-DSS	5	9.5 Store media back-ups in a secure location, preferably an offsite facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	N			
PCI	9	6	PCI.9.6	PCI-DSS	5	9.6 Physically secure all media.	N			
PCI	9	7	PCI.9.7	PCI-DSS	5	9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	N			
PCI	9	7.1	PCI.9.7.1	PCI-DSS	5	9.7.1 Classify media so the sensitivity of the data can be determined.	N			
PCI	9	7.2	PCI.9.7.2	PCI-DSS	5	9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	N			
PCI	9	8	PCI.9.8	PCI-DSS	5	9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	N			
PCI	9	9	PCI.9.9	PCI-DSS	5	9.9 Maintain strict control over the storage and accessibility of media.	N			
PCI	9	9.1	PCI.9.9.1	PCI-DSS	5	9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	N			
PCI	9	10	PCI.9.10	PCI-DSS	1	9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	N			
PCI	9	10.1	PCI.9.10.1	PCI-DSS	1	9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	N			
PCI	9	10.2	PCI.9.10.2	PCI-DSS	1	9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	N			
PCI	10	0	PCI.10.0	PCI-DSS		Requirement 10: Track and monitor all access to network resources and cardholder data	N			
PCI	10	1	PCI.10.1	PCI-DSS	4	10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	N			
PCI	10	2	PCI.10.2	PCI-DSS	4	10.2 Implement automated audit trails for all system components to reconstruct the following events:	N			
PCI	10	2.1	PCI.10.2.1	PCI-DSS	4	10.2.1 All individual accesses to cardholder data.	N			
PCI	10	2.2	PCI.10.2.2	PCI-DSS	4	10.2.2 All actions taken by any individual with root or administrative privileges.	N			
PCI	10	2.3	PCI.10.2.3	PCI-DSS	4	10.2.3 Access to all audit trails.	N			
PCI	10	2.4	PCI.10.2.4	PCI-DSS	4	10.2.4 Invalid logical access attempts.	N			
PCI	10	2.5	PCI.10.2.5	PCI-DSS	4	10.2.5 Use of identification and authentication mechanisms.	N			
PCI	10	2.6	PCI.10.2.6	PCI-DSS	4	10.2.6 Initialization of the audit logs.	N			
PCI	10	2.7	PCI.10.2.7	PCI-DSS	4	10.2.7 Creation and deletion of system-level objects.	N			
PCI	10	3	PCI.10.3	PCI-DSS	4	10.3 Record at least the following audit trail entries for all system components for each event:	N			
PCI	10	3.1	PCI.10.3.1	PCI-DSS	4	10.3.1 User identification.	N			
PCI	10	3.2	PCI.10.3.2	PCI-DSS	4	10.3.2 Type of event.	N			
PCI	10	3.3	PCI.10.3.3	PCI-DSS	4	10.3.3 Date and time.	N			
PCI	10	3.4	PCI.10.3.4	PCI-DSS	4	10.3.4 Success or failure indication.	N			
PCI	10	3.5	PCI.10.3.5	PCI-DSS	4	10.3.5 Origination of event.	N			
PCI	10	3.6	PCI.10.3.6	PCI-DSS	4	10.3.6 Identity or name of affected data, system component, or resource.	N			
PCI	10	4	PCI.10.4	PCI-DSS	4	10.4 Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	N			
PCI	10	4.1	PCI.10.4.1	PCI-DSS	4	10.4.1 Critical systems have the correct and consistent time.	N			
PCI	10	4.2	PCI.10.4.2	PCI-DSS	4	10.4.2 Time data is protected.	N			
PCI	10	4.3	PCI.10.4.3	PCI-DSS	4	10.4.3 Time settings are received from industry-accepted time sources.	N			
PCI	10	5	PCI.10.5	PCI-DSS	4	10.5 Secure audit trails so they cannot be altered.	N			
PCI	10	5.1	PCI.10.5.1	PCI-DSS	4	10.5.1 Limit viewing of audit trails to those with a job-related need.	N			
PCI	10	5.2	PCI.10.5.2	PCI-DSS	4	10.5.2 Protect audit trail files from unauthorized modifications.	N			
PCI	10	5.3	PCI.10.5.3	PCI-DSS	4	10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	N			
PCI	10	5.4	PCI.10.5.4	PCI-DSS	4	10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	N			
PCI	10	5.5	PCI.10.5.5	PCI-DSS	4	10.5.5 Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	N			
PCI	10	6	PCI.10.6	PCI-DSS	4	10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).	N			
PCI	10	7	PCI.10.7	PCI-DSS	4	10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	N			
PCI	11	0	PCI.11.0	PCI-DSS		Requirement 11: Regularly test security systems and processes	N			

PCI	11	1	PCI.11.1	PCI-DSS	4	11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.	N			
PCI	11	2	PCI.11.2	PCI-DSS	2	11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	N			
PCI	11	2.1	PCI.11.2.1	PCI-DSS	2	11.2.1 Perform quarterly internal vulnerability scans.	N			
PCI	11	2.2	PCI.11.2.2	PCI-DSS	2	11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).	N			
PCI	11	2.3	PCI.11.2.3	PCI-DSS	2	11.2.3 Perform internal and external scans after any significant change.	N			
PCI	11	3	PCI.11.3	PCI-DSS	2	11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	N			
PCI	11	3.1	PCI.11.3.1	PCI-DSS	2	These penetration tests must include the following:11.3.1 Network-layer penetration tests.	N			
PCI	11	3.2	PCI.11.3.2	PCI-DSS	2	11.3.2 Application-layer penetration tests.	N			
PCI	11	4	PCI.11.4	PCI-DSS	2	11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up-to-date.	N			
PCI	11	5	PCI.11.5	PCI-DSS	4	11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.	N			
PCI	12	0	PCI.12.0	PCI-DSS		Requirement 12: Maintain a policy that addresses information security for all personnel	N			
PCI	12	1	PCI.12.1	PCI-DSS	6	12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	N			
PCI	12	1.1	PCI.12.1.1	PCI-DSS	6	12.1.1 Addresses all PCI-DSS requirements	N			
PCI	12	1.2	PCI.12.1.2	PCI-DSS	1	12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	N			
PCI	12	1.3	PCI.12.1.3	PCI-DSS	6	12.1.3 Includes a review at least annually and updates when the environment changes.	N			
PCI	12	2	PCI.12.2	PCI-DSS	6	12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	N			
PCI	12	3	PCI.12.3	PCI-DSS	6	12.3 Develop usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email usage and internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	N			
PCI	12	3.1	PCI.12.3.1	PCI-DSS	6	12.3.1 Explicit approval by authorized parties.	N			
PCI	12	3.2	PCI.12.3.2	PCI-DSS	6	12.3.2 Authentication for use of the technology.	N			
PCI	12	3.3	PCI.12.3.3	PCI-DSS	6	12.3.3 A list of all such devices and personnel with access.	N			
PCI	12	3.4	PCI.12.3.4	PCI-DSS	6	12.3.4 Labeling of devices to determine owner, contact information, and purpose.	N			
PCI	12	3.5	PCI.12.3.5	PCI-DSS	6	12.3.5 Acceptable uses of the technology.	N			
PCI	12	3.6	PCI.12.3.6	PCI-DSS	6	12.3.6 Acceptable network locations for the technologies.	N			
PCI	12	3.7	PCI.12.3.7	PCI-DSS	6	12.3.7 List of company-approved products.	N			
PCI	12	3.8	PCI.12.3.8	PCI-DSS	6	12.3.8 Automatic disconnect of sessions for remote access technologies after a specific period of inactivity.	N			
PCI	12	3.9	PCI.12.3.9	PCI-DSS	6	12.3.9 Activation of remote access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	N			
PCI	12	3.10	PCI.12.3.10	PCI-DSS	6	12.3.10 For personnel accessing cardholder data via remote access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	N			
PCI	12	4	PCI.12.4	PCI-DSS	6	12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	N			
PCI	12	5	PCI.12.5	PCI-DSS	6	12.5 Assign to an individual or team the following information security management responsibilities:	N			
PCI	12	5.1	PCI.12.5.1	PCI-DSS	6	12.5.1 Establish, document, and distribute security policies and procedures.	N			
PCI	12	5.2	PCI.12.5.2	PCI-DSS	6	12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	N			
PCI	12	5.3	PCI.12.5.3	PCI-DSS	4	12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	N			
PCI	12	5.4	PCI.12.5.4	PCI-DSS	6	12.5.4 Administer user accounts, including additions, deletions, and modifications.	N			
PCI	12	5.5	PCI.12.5.5	PCI-DSS	6	12.5.5 Monitor and control all access to data.	N			
PCI	12	6	PCI.12.6	PCI-DSS	6	12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	N			
PCI	12	6.1	PCI.12.6.1	PCI-DSS	6	12.6.1 Educate personnel upon hire at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	N			
PCI	12	6.2	PCI.12.6.2	PCI-DSS	6	12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	N			
PCI	12	7	PCI.12.7	PCI-DSS	6	12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	N			
PCI	12	8	PCI.12.8	PCI-DSS	2	12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	N			
PCI	12	8.1	PCI.12.8.1	PCI-DSS	2	12.8.1 Maintain a list of service providers.	N			
PCI	12	8.2	PCI.12.8.2	PCI-DSS	2	12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	N			
PCI	12	8.3	PCI.12.8.3	PCI-DSS	2	12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	N			
PCI	12	8.4	PCI.12.8.4	PCI-DSS	2	12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	N			
PCI	12	9	PCI.12.9	PCI-DSS	4	12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	N			

PCI	12	9.1	PCI.12.9.1	PCI-DSS	4	12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: § Roles, responsibilities and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum § Specific incident response procedures § Business recovery and continuity procedures § Data back-up processes § Analysis of legal requirements for reporting compromises § Coverage and responses of all critical system components § Reference or inclusion of incident response procedures from the payment brands	N			
PCI	12	9.2	PCI.12.9.2	PCI-DSS	4	12.9.2 Test the plan at least annually.	N			
PCI	12	9.3	PCI.12.9.3	PCI-DSS	4	12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	N			
PCI	12	9.4	PCI.12.9.4	PCI-DSS	4	12.9.4 Provide appropriate training to staff with security breach response responsibilities.	N			
PCI	12	9.5	PCI.12.9.5	PCI-DSS	4	12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	N			
PCI	1	9.6	PCI.1.9.6	PCI-DSS	4	12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	N			
PCI	A	1	PCI.A.1	PCI-DSS	3	Requirement A.1: Shared hosting providers must protect the cardholder data environment. A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS	N			
PCI	A	1.1	PCI.A.1.1	PCI-DSS	3	A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	N			
PCI	A	1.2	PCI.A.1.2	PCI-DSS	3	A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	N			
PCI	A	1.3	PCI.A.1.3	PCI-DSS	3	A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	N			
PCI	A	1.4	PCI.A.1.4	PCI-DSS	3	A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	N			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Service Oriented Architecture (SOA)

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN1	1	1	SLN1.1.1	SOA General		Solutions components shall be committed to an advanced approach to interoperability using web services and Service Oriented Architecture (SOA) aligned with State standards and vision for interoperability.	Y		
SLN1	1	2	SLN1.1.2	SOA General		Solutions shall implement a Service Oriented Architecture by using an Enterprise Service Bus, responsible to monitor and control routing of message exchange between services, resolve contention between communicating service components, control deployment and versioning of services and marshal use of redundant services.	Y		
SLN1	1	3	SLN1.1.3	SOA General		Solutions shall support creation and extension of service interfaces through the use of Web Services Description Language (WSDL)	Y		
SLN1	1	4	SLN1.1.4	SOA General		Solutions shall provide the ability to distribute services amongst different components and tiers of the architecture.	Y		
SLN1	1	5	SLN1.1.5	SOA General		Solutions shall develop/integrate services using standardized Web Services formats.	Y		
SLN1	1	6	SLN1.1.6	SOA General		Solutions shall allow for centralized service maintenance (new, update, delete).	Y		
SLN1	1	7	SLN1.1.7	SOA General		Solutions shall provide the ability to publish services and related data to be used by different types and classes of service consumers.	Y		
SLN1	1	8	SLN1.1.8	SOA General		Solutions shall ensure enterprise-wide access to services through all required channels.	Y		
SLN1	1	9	SLN1.1.9	SOA General		Solutions shall provide the capabilities for a Real-Time (or near real-time) Integrated Enterprise where common data elements about the consumers served and services rendered are easily shared across organizational units with appropriate adherence to security and privacy restrictions.	Y		
SLN1	1	10	SLN1.1.10	SOA General		Solutions shall establish an interoperability layer that supports interactions among components via a variety of protocols (HTTP/plain old XML [POX], SOAP, Internet Inter-ORB Protocol [IIOP], .NET remoting, Message-Oriented Middleware [MOM] protocols, file transfer protocols and others) and interaction styles (request/reply, conversational, publish and subscribe, asynchronous messaging and others).	Y		
SLN1	1	11	SLN1.1.11	SOA General		Solutions shall implement synchronous and asynchronous program-to-program communication, moving messages between SOA service consumer modules and service provider modules at runtime. The ESB component may also move files, database rows and other data.	Y		
SLN1	1	12	SLN1.1.12	Logical Data Representation		Message and data formats should be based on logical representations of business objects rather than native application data structures	Y		
SLN1	1	13	SLN1.1.13	Normalized Data Formats		Data transformations shall be to and from normalized formats. Normalized data formats facilitate composition and reduce the number of transformations that must be created and maintained. A canonical data representation that spans the enterprise can be used but is not required. A federated approach to data normalization is also possible	Y		
SLN1	1	14	SLN1.1.14	Avoid Point-to-Point Integrations		Point-to-point integrations are to be avoided. Application integration, both internal and external, shall go through the central ESB. Point-to-point integrations are brittle, inflexible, and expensive to maintain. There are cases where point-to-point integrations are required but these should be handled as exception cases. Example exceptions include performance requirements that can only be met using point-to-point connections and when large amounts of data must be moved	Y		
SLN1	1	15	SLN1.1.15	Technical Orchestration		Technical orchestration shall be separated from business processes. Making a clear distinction between technical aspects and business aspects facilitates maintenance of both. Technical aspects change when the underlying systems change whereas business aspects change when the business changes	Y		
SLN1	1	16	SLN1.1.16	Business-level Services		SOA Services shall expose business-level functionality and data. Business-level functionality and data are required to create business valuable composite applications. There may also be lower-level SOA Services that are reused by the business-level SOA Services.	Y		
SLN1	1	17	SLN1.1.17	Service Contract		SOA Services include a contract that specifies the functional and non-functional capabilities provided. In order to support business-level composition, the SOA Service must have a contract that is understandable to a business person	Y		
SLN1	1	18	SLN1.1.18	Access via Services		Enterprise data and functions shall be accessed through SOA Services. SOA Services create the foundation for agile composite application development. Failing to leverage SOA Services defeats the primary goal of service-oriented integration	Y		
SLN1	1	19	SLN1.1.19	Opaque Service Implementation		The implementation of a SOA Service is opaque to all service consumers. Service consumers must be able to successfully call a SOA Service without needing to understand the internal workings of the SOA Services.	Y		
SLN1	1	20	SLN1.1.20	Platform Independence		The service consumer platform is independent from the service provider platform. SOA Services need to support any kind of service consumer regardless of the particular platform that the consumer is built upon	Y		

SLN1	1	21	SLN1.1.21	Location Transparency		The location of a service provider is unimportant to the service consumer and vice-versa Location transparency helps provide the de-coupling of service consumers and providers necessary for extensive SOA Service reuse	provider is unimportant to the service consumer (assuming the service can detect and apply the relivant security protocols that may apply based on the origination location)		
SLN1	1	22	SLN1.1.22	Concurrent Service Versions		Service design, implementation, and consumption shall support multiple versions of a SOA Service in production concurrently.	Y		
SLN1	1	23	SLN1.1.23	Graceful Service Migration		Service consumers shall be able to migrate to a newer version of a SOA Service gracefully. Service consumers should migrate to a new version of a SOA Service as part of a normal maintenance process. The coordinated deployment of service consumers and service providers should not be necessary	Y		
SLN1	1	24	SLN1.1.24	Event Processing		Applications included in the integration can raise events which must be processed consistently. Events allow the applications that are included in the integration to notify other applications that something important has occurred. The events that are raised by applications must not be ignored and the architecture should handle the events in a consistent manner. Each event should trigger the appropriate response.	Y		
SLN1	1	25	SLN1.1.25	Service Classification		All services shall be classified with one of the following values: Presentation, Process, Business, Data, Access, or Utility	Y		
SLN1	1	26	SLN1.1.26	Service Portfolio Management		All services shall be reviewed, classified, and cataloged prior to use. Duplicate services shall be rationaled and retired appropriately	Y		
SLN1	1	27	SLN1.1.27	Service Ownership		All services shall have key stakeholder/owners identified	Y		
SLN1	1	28	SLN1.1.28	WSDL Development Standards		All WSDLs developed for Vermont shall conform to the WSDL Development Standards	Y		
SLN1	1	29	SLN1.1.29	XSD Standardization		All SOA-related messages shall be formally defined with XSD (preferable) or DTDs.	Y		
SLN1	1	30	SLN1.1.30	SOA Service Language		SOA-related services hosted should be implemented in Java.	Y		
SLN1	1	31	SLN1.1.31	SOA policy		Implemented services shall rely on WS-Policy configurations for message reliability (WS-ReliableMessaging)	Y		
SLN1	1	32	SLN1.1.32	SOA Metadata		The following metadata attributes shall be tracked for all services in the services catalog: {name, lifecycle status, class, description, owner, version, revision history, release frequency, versioning policy, deprecation policy, message exchange patterns, compensating transaction support, availability requirements, volume, max message size, security attributes, sla, logging requirements}	Y		
SLN1	1	33	SLN1.1.33	SOA Lifecycle Status		SOA services shall be attributed with one of the following SOA Lifecycle Status values: Candidate, Justified, Defined, Designed, Implemented, Operational, or Retired.	Y		
SLN1	1	34	SLN1.1.34	Central SOA Component Deployment		The service bus, registry, and repository shall be deployed as one logical entity in production instead of federating for each agency. SOA component federation shall not be permitted.	Y		
SLN1	1	35	SLN1.1.35	SOA IdM Integration		SOA technology components shall rely on the central IdM technology components for authentication/authorization	Y		
SLN1	1	36	SLN1.1.36	SOA Rules Integration		Business rules implemented with the rules engine should be accessed through a SOA service	Y		
SLN1	1	37	SLN1.1.37	SOA General		Be designed, built and deployed with enterprise architecture best practices including substantial reliance on highly configurable SOA components.	Y		
SLN1	1	38	SLN1.1.38	SOA General		Solutions shall provide reliable, once-only delivery of messages (guarantee of reliable and non-repetitive delivery).	Y		
SLN1	1	39	SLN1.1.39	SOA General		Solutions shall support the industry-standards messaging and interfaces relevant to health and human services organizations including, but not limited to: - Health Level Seven (HL7) Versions 2.x, 3.x, and CCD - Integrating the Healthcare Enterprise (IHE) XD* Profiles	Yes; including Electomic Data Inerchange (EDI) X12 healthcare format		
SLN1	1	40	SLN1.1.40	SOA General		Solutions shall provide the technology that hosts the execution of process logic spanning multiple back-end services or applications - typically for short-term (seconds or minutes) processes that can occasionally also be long term (hours, days, weeks) - with the aim of implementing composite services or automated solution-to-Solution processes. Features include: ' Graphical design surface for specifying process flows ' Support for standard specification languages including Business Process Modeling Notation (BPMN) ' Support for standard representations including Business Process Execution Language (BPEL), XML Process Definition Language (XPDL), Business Process Modeling Language (BPML) and Web Services Flow Language (WSFL) ' Ability to specify compensating transactions and execute those transactions upon failure of the process flow ' Integration with workflow	Y		

SLN1	1	41	SLN1.1.41	SOA General		Solutions shall provide the technology to perform syntactic and semantic hub-based transformation of messages, including: ' Support of taxonomy ' Support of ontology ' Reusable transformation maps ' Built-in transformation functions ' Extending the transformation function with custom-coded logic ' Support B2B project translation including Electronic Data Interchange (EDI), RosettaNet, HL7, etc.	Y		
SLN1	1	42	SLN1.1.42	SOA General		Solutions shall provide the functionality that provides reliability for applications, services or message flows: ' Load balancing ' High availability ' Fault tolerance ' Failover ' In-order delivery ' Transaction support ' Execution prioritization ' Message prioritization	Y		
SLN1	1	43	SLN1.1.43	SOA General		Solutions shall provide the functionality used to monitor the operation of the overall Solution (services, applications, processes and application infrastructure), and to collect events and usage information aimed at populating technical KPIs of the deliverables supported by the SOA backplane and of the SOA backplane components by monitoring and collecting metrics for: ' Messaging traffic ' Process state and behavior ' Application and service parameters and behavior for all nodes in a LAN or WAN	Y		
SLN1	1	44	SLN1.1.44	SOA General		Solutions shall provide the tools and technologies required to implement the necessary control access to the services and the connected resources (for example, other services and databases), as well as the SOA backplane functionality. Capabilities include: ' Authentication ' Authorization ' Encryption/decryption ' Digital signatures ' Credential mapping	Y		
SLN1	1	45	SLN1.1.45	SOA General		Solutions shall provide the functionality to assist State's operations personnel in keeping the resultant Solution (applications, services and infrastructure) running at peak efficiency at all times, including: ' Establishing rules for automated Solution monitoring ' Establishing network-alert-based management ' Supporting autonomous network behavior so local management and problem Resolution can continue during an outage ' A console that enables domain-specific display for multiple devices	Y		
SLN1	1	46	SLN1.1.46	SOA General		Solutions shall provide the technology that manages the metadata and provides the features needed to support the reliable operation of services. Examples include: ' Online catalog of services and associated artifacts such as WSDL files, XSDs, BPEL files ' A single point of controlled access for cataloging, promoting, publishing and searching for information about managed assets ' Metadata that enables an Enterprise Service Bus (ESB) to find, bind to and invoke the execution of a service implementation ' Support for extending existing asset types and defining and populating custom asset types	Y		
SLN1	1	47	SLN1.1.47	SOA General		Solutions shall provide support for building frameworks and extensible tools that enable the design, configuration, assembly, deployment, monitoring, and management of software designed around an SOA.	Y		
SLN1	1	48	SLN1.1.48	SOA General		Solutions shall provide assistance for deploying applications with SOA and event-driven architecture in a manner that supports the following implementation strategies: ' Web Services: Web Services Interoperability (WS-I) Organization-compliant implementation of basic Web services standards, including SOAP, WSDL and Universal Description, Discovery and Integration (UDDI), as well as higher-level Web services standards, such as WS-Security. ' Representational State Transfer (REST): Support for XML-based messages, processing and HTTP, and XHTML.	Y		
SLN1	1	49	SLN1.1.49	SOA General		Solutions shall have the ability to support varying message payloads, ranging from individual transactions to large files (more than 1GB) containing multiple transactions.	Yes, the SOA solution shall be configurated to approproate manage these varying types of message construrtion and size thorugh a common set of components. Where possible, solutions should error on the side of individual transactions per message to simplify the message management, routing, and database recovery needs.		
SLN1	1	50	SLN1.1.50	SOA General		Solutions shall provide the technology to implement processing logic that directly manipulates data values, and the representation of those values for storage, transport or presentation purposes. This processing logic is used to establish common access to data sources (structured and unstructured), improve data quality or federate data from multiple sources.	Y		

SLN1	1	51	SLN1.1.51	SOA General		Solutions shall provide the tooling that enables the recording (storage) or retrieving (reading) of information (data) from data stores. An example is distributed query functionality that parses incoming queries into sub queries and the execution of those sub queries, via the connectivity layer, against the respective sources where the desired data resides.	Y		
SLN1	1	52	SLN1.1.52	SOA General		Solutions shall provide the data infrastructure tooling that enables users to represent semantic models, identify model-to-model relationships, and execute the necessary translations to reconcile data with differing semantic models.	Y		
SLN1	1	53	SLN1.1.53	SOA General		Solutions shall provide optimization services that continuously read various types of metadata from across the architecture. The optimization verbs shall use the semantic/logical services to reconcile context to data content and deliver against some aspect of the application service-level agreement (requirements for data quality, data freshness, data volumes, throughput parameters, data-mining results, on-demand data aggregation or summarization, data enrichment, and many others).	Y		
SLN1	1	54	SLN1.1.54	SOA General		Solutions shall provide tooling that supports data profiling: the process of examining the data available in an existing data source (for example, a database or a file), and collecting statistics and information about that data. The purpose of these statistics may be to: ' Find out whether existing data can easily be used for other purposes. ' Give metrics on data quality, including whether the data conforms to company standards. ' Assess the risk involved in integrating data for new applications. ' Track data quality. ' Assess whether metadata accurately describes the actual values in the source database. ' Establish an understanding of data challenges early in any data-intensive project, so that late project surprises are avoided. Finding data problems late in the project can incur time delays and project cost overruns. ' Have an enterprise view of all data for uses such as master data management (MDM), where key data is needed, or data governance, for improving data quality.	Y		
SLN1	1	55	SLN1.1.55	SOA General		Solutions shall provide a modeling environment to support the roles of the business analyst, process architect, Solution architect and developer. It enables the modeling and architecture of all process artifacts.	Y		
SLN1	1	56	SLN1.1.56	SOA General		Solutions shall support individual and group teamwork at design time and runtime.	Y		
SLN1	1	57	SLN1.1.57	SOA General		Solutions shall have the ability to track a message from its origin to its destination (inside a firewall), inquire on the status of that message and address exceptions (for example, resend the message if a target times out). Usually implemented via a warehouse for archiving messages together with the associated tracking and logging data.	Yes: full transational "functional" SAGA will be tracked.		
SLN1	1	58	SLN1.1.58	SOA General		The Solution must incorporate Role/Group-based rights for the management of the Service Bus across the environments.	Y		
SLN1	1	59	SLN1.1.59	SOA General		Solutions shall have: ' Protocols: The ability to use standards-based communication protocols, such as TCP/IP, HTTP, HTTP/S and SMTP. ' Protocol bridging: The ability to convert between the protocol native to the messaging platform and other protocols, such as Remote Method Invocation (RMI), IIOP and .NET remoting.	Y		
SLN1	1	60	SLN1.1.60	SOA General		Solutions shall have features that enable in-flight message manipulation, such as transformation (typically XML-based), intelligent routing, naming and addressing.	Y		
SLN1	1	61	SLN1.1.61	SOA General		Solutions shall have the ability to apply logic to the routing of messages, including support for the following file interaction styles: ' Store and forward: Ability to persist a message and then send it to destinations. ' Publish/subscribe: Ability to distribute a message to multiple destinations based on a message attribute usually described as the subject area of the message. ' Request/reply: Ability to correlate asynchronous messages so that the target's response is associated with the appropriate request made by the source. ' Content-based: The ability to route a message based on a value or values within a message. For example, the ability to route a referral message whose target turnaround time is small to a different set of targets than a referral message whose turnaround time is high.	Y		
SLN1	1	62	SLN1.1.62	SOA General		Solutions shall provide for syntactic conversion and semantic transformation, including ease of use and reuse, number of built-in functions, ease of extending the transformation function with custom-coded logic and XML support (e.g. schema or Extensible Stylesheet Language Transformations [XSLT]).	Y		
SLN1	1	63	SLN1.1.63	SOA General		Solutions shall have the capability during operations, to assist service consumers by dynamically finding, binding to and invoking the execution of service providers.	Y		
SLN1	1	64	SLN1.1.64	SOA General		Solutions shall provide the technology that combines design tools and runtime software to implement programs that act as glue, transforming among protocols, connecting to databases and linking pre-SOA Application Programming Interfaces (APIs) to the SOA backplane. To support B2B projects, adapters also need to support SOA services using B2B protocols such as Applicability Statement 1 (AS1)/Applicability Statement 2 (AS2), RosettaNet and Electronic Data Interchange for Administration, Commerce and Transportation (EDIFACT).	Y		
SLN1	1	65	SLN1.1.65	SOA General		An Enterprise Metadata Repository shall provide design-time governance in support of the service lifecycle, delivering key capabilities for the storage and management of an extensible set of metadata for number of composites, services, business processes, and other IT-related assets	Y		
SLN1	1	66	SLN1.1.66	SOA General		A Service Registry shall serve as an integration point for runtime tooling	Y		
SLN1	1	67	SLN1.1.67	SOA General		Service Bus shall subscribe to new or modified assets	Y		
SLN1	1	68	SLN1.1.68	SOA General		Composite applications shall discover updated endpoints and WSDL locations	Y		
SLN1	1	69	SLN1.1.69	SOA General		Runtime monitoring tooling shall publish metrics to the Service Registry	Y		
SLN1	1	70	SLN1.1.70	SOA General		Security policy manager for Web services that allows for centrally defined security policies that govern Web services operations (such as access policy, logging policy, and load balancing)	Y		
SLN1	1	71	SLN1.1.71	SOA General		Shall provide dynamic discovery and service level monitoring of all artifacts deployed in the Application Server	Y		
SLN1	1	72	SLN1.1.72	SOA General		Project teams (vendor-supplied or otherwise) shall define governance processes for the following domains:1. Service Portfolio Mgmt, 2. Services Technical Arch, 3. Service Design & Dev, 4. Configuration & Release Mgmt, 5. Contract Mgmt, 6. Service Monitoring & Control, 7. Incident Mgmt, 8. Change Mgmt	Y		

SLN1	1	73	SLN1.1.73	SOA General		These SOA guidelines are to provide consistency, enable a framework for SOA govrenance, simpify development, and improve operations. However, at times exceptions to these guidelines maybe necessary to satisfy a specific functional or technical needs. When this occurs, approrpaite SOA governance policies and processes will drive the steps.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Audit

Base	Level	Sub	Req ID New	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN2	1	1	SLN2.1.1	Audit General		Solutions shall maintain a record (e.g. audit trail) of all additions, changes and deletions made to data in the system. This should be readily searchable by user ID or client ID. This must include but is not limited to: - The user ID of the person who made the change - The date and time of the change - The physical, software/hardware and/or network location of the person while making the change - The information that was changed - The outcome of the event - The data before and after it was changed, and which screens were accessed and used	Y		
SLN2	1	2	SLN2.1.2	Audit General		Solutions shall prevent modifications to the audit records.	Yes: Solutions shall prevent modifications to the audit records, in the normal course of operations. Any change or removal of an audit record would require signed leadership approval and would be documented.		
SLN2	1	3	SLN2.1.3	Audit General		The proposed Solution must provide logging, reporting and accessing errors and exceptions.	Y		
SLN2	1	4	SLN2.1.4	Audit General		Solutions shall provide capability for integrating consent audit trails and data access audit trails in a consolidated report to support consent rule enforcement or investigation including audit trails based on deprecated rules or policies.	Y		
SLN2	1	5	SLN2.1.5	Audit General		Solutions shall generate and protect consent audit events at the same or better levels as other data access audit records.	Y		
SLN2	1	6	SLN2.1.6	Audit General		Solutions shall allow an authorized administrator to set the inclusion or exclusion of auditable events based on organizational policy & operating requirements/limits.	Y		
SLN2	1	7	SLN2.1.7	Audit General		Solutions shall support logging to a common audit engine using the schema and transports specified in the Integrating the Healthcare Enterprise (IHE) Audit Trails and Node Authentication (ATNA) profile, Audit Log specification.	Y		
SLN2	1	8	SLN2.1.8	Audit General		Solutions shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include those listed here: - start/stop - user login/logout - session timeout - account lockout - client record created/viewed/updated/deleted - scheduling - query - order - node-authentication failure - signature created/validated - Personally Identifiable Information (PII) export - PII import - security administration events - backup and restore	Y		
SLN2	1	9	SLN2.1.9	Audit General		Solutions shall provide authorized administrators with the capability to read all audit information from the audit records in the following two ways: 1) Solutions shall provide the audit records in a manner suitable for the user to interpret the information. Solutions shall provide the capability to generate reports based on ranges of Solution date and time that audit records were collected. 2) Solutions shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. Coordinated Universal Time [UTC] synchronization).	Y		
SLN2	1	10	SLN2.1.10	Audit General		Solutions shall be able to perform time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.	Y		
SLN2	1	11	SLN2.1.11	Audit General		Solutions shall have the ability to format for export recorded time stamps using UTC based on ISO 8601.	Y		
SLN2	1	12	SLN2.1.12	Audit General		Solutions shall prohibit all users read access to the audit records, except those users that have been granted explicit read access.	Y		
SLN2	1	13	SLN2.1.13	Audit General		Solutions shall protect the stored audit records from unauthorized modification or deletion. Solutions shall prevent modifications to the audit records.	Y		
SLN2	1	14	SLN2.1.14	Audit General		Provide the ability to audit and log the network system/application and detailed user activity including data available to the user, data viewed by user, data downloaded by user, data uploaded by the solution, and all actions taken by user while in the system) in accordance with policy defined by the Exchange.	Y	Auditing	
SLN2	1	15	SLN2.1.15	Audit General		Provide and retain transaction logs in accordance with the National Institute of Standards and Technology (NIST) requirements.	Y	Auditing	
SLN2	1	16	SLN2.1.16	Audit General		Provide and retain transaction logs in accordance with the Health Insurance Portability and Accountability Act (HIPAA).	Y	Auditing	
SLN2	1	17	SLN2.1.17	Audit General		Provide and retain transaction logs in accordance with the Harmonized Security and Privacy Framework.	Y	Auditing	
SLN2	1	18	SLN2.1.18	Audit General		Provide reporting for security audits and compliance activities based on designated timeframes.	Y	Auditing	
SLN2	1	19	SLN2.1.19	Audit General		Provide ability to set security controls for audit logs via role based access controls.	Y	Auditing	
SLN2	1	20	SLN2.1.20	Audit General		Provide flexible audit report function (including on demand feature) and audit logging ability.	Y	Auditing	

SLN2	1	21	SLN2.1.21	Audit General		Provide ability to perform the database capabilities to facilitate audit.	Y	Auditing	
SLN2	1	22	SLN2.1.22	Audit General		The Contractor shall support an audit of data center operations by a 3rd party vendor, including, but not limited to: SSAE-16, Pentration Test, etc.	Y	Auditing	
SLN2	1	23	SLN2.1.23	Audit General		The Contractor shall provide the ability for the Exchange to examine system and error daily logs to minimize and predict system problems and initiate appropriate action.	Y	Auditing	
SLN2	1	24	SLN2.1.24	Audit General		Audit records will be date / Time stamped using Coordinated Universal Time [UTC]. Time will be tracked at the hundreth of a second (minimum).	Y	Auditing	

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Business Intelligence & Extract, Transfer & Load

Base	Level	Sub.	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN3	1	1	SLN3.1.1	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide scalable architecture and support design that will provide flexibility to add more data fields and change granularity level efficiently as analytic demand matures and expands.	Y		
SLN3	1	2	SLN3.1.2	Business Intelligence General		Shared Analytics Infrastructure Solutions shall have the ability to capture delta change of data from diverse systems and populate them to Shared Analytics.	Y		
SLN3	1	3	SLN3.1.3	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide the ability to capture and load data via Service Oriented Architecture (SOA)-based services and the ability to schedule data integration and load jobs.	Y		
SLN3	1	4	SLN3.1.4	Business Intelligence General		Shared Analytics Infrastructure Solutions shall include the ability to facilitate design and construction of data integration processes.	Y		
SLN3	1	5	SLN3.1.5	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide the ability to create custom transformations and the ability to group and reuse mapping and transformation operations.	Y		
SLN3	1	6	SLN3.1.6	Business Intelligence General		Solutions shall support multi-dimensional views and multidimensional tables.	Y		
SLN3	1	7	SLN3.1.7	Business Intelligence General		Shared Analytics Infrastructure Solutions shall have the ability to support physical creation and storage of views as well as logical view.	Y		
SLN3	1	8	SLN3.1.8	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support design to facilitate a single view of business data.	Y		
SLN3	1	9	SLN3.1.9	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support Online Analytical Processing (OLAP) database structure for use in analytics and business intelligence.	Y		
SLN3	1	10	SLN3.1.10	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support hierarchical drill up/down; ad-hoc query; multi-dimensional view and multidimensional table.	Y		
SLN3	1	11	SLN3.1.11	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide the ability to support data mining functions.	Y		
SLN3	1	12	SLN3.1.12	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide the ability to perform in-database analytics.			
SLN3	1	13	SLN3.1.13	Business Intelligence General		Shared Analytics Infrastructure Solutions shall offer options to use Database Management Solution (DBMS)-integrated data integration tool and/or third party vendor integration tool.	Y		
SLN3	1	14	SLN3.1.14	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support fast large volume data loading and shall have the ability to capture real-time data.	Y		
SLN3	1	15	SLN3.1.15	Business Intelligence General		Solutions shall provide the ability to impose graduated access to reports based on user role and agency requirements/permissions to better analyze program data.	Y		
SLN3	1	16	SLN3.1.16	Business Intelligence General		The Solution's business intelligence and reporting capabilities must be scalable to accommodate changes in Solution scale including changes in user population, transaction volume, throughput and geographical distribution while maintaining the agreed service levels.	Y		
SLN3	1	17	SLN3.1.17	Business Intelligence General		Solutions shall have a mechanism to share specific data (e.g. limited data sets, detailed data at the level of the individual but with the data anonymous and completely de-identified, etc.) in a controllable fashion with other State and local agencies.	Y		
SLN3	1	18	SLN3.1.18	Business Intelligence General		Solutions shall be extensible and have a scalable data architecture incorporating State and external data.	Y		
SLN3	1	19	SLN3.1.19	Business Intelligence General		Solutions shall provide a tool to allow predictive modeling and analysis utilizing production data and coexist and integrate with such tools already in use (SPSS and SAS).	N		
SLN3	1	20	SLN3.1.20	Business Intelligence General		Solutions shall provide the ability for user to create and customize reports, queries, and dashboards.	Y		
SLN3	1	21	SLN3.1.21	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide comprehensive metadata management from source to target.	Y		
SLN3	1	22	SLN3.1.22	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide single repository for metadata, such as mappings of business concepts to underlying data structures, business glossary, data lineage, reference data, and objects (e.g. view, table, join) and reports from source to target.	Y		
SLN3	1	23	SLN3.1.23	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide the ability to import metadata from tools and data sources.	Y		
SLN3	1	24	SLN3.1.24	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide data quality tool or support 3rd party data quality tool for profiling, cleansing, and monitoring.	Y		
SLN3	1	25	SLN3.1.25	Business Intelligence General		Shared Analytics Infrastructure Solutions shall produce metadata and/or data dictionaries in a format that the State can consume, e.g., Word, Excel, PDF, OF, etc.	Y		
SLN3	1	26	SLN3.1.26	Business Intelligence General		Shared Analytics Infrastructure Solutions shall be highly available via various mechanisms. (e.g. data mart. Data replication, Tool provided for management of high availability, cluster option, back up configuration).	Y		
SLN3	1	27	SLN3.1.27	Business Intelligence General		Shared Analytics Infrastructure Solutions shall have an option for fast loading of data into the database. Where necessary this will include minimal relaxation of quality and integrity constraints and mechanisms for carrying out data quality checks as the final stage in the process.	Y		

SLN3	1	28	SLN3.1.28	Business Intelligence General		Solutions shall provide for expansion of data storage as needed to accommodate increased volume of data based on approved Capacity Plans by the State.	Y		
SLN3	1	29	SLN3.1.29	Business Intelligence General		Shared Analytics Infrastructure Solutions shall be American National Standards Institute (ANSI) Structured Query Language (SQL) Compliant. (Vendrs/data sheets need to specify version of SQL compliant ' e.g. 2003, 2006, 2008).			
SLN3	1	30	SLN3.1.30	Business Intelligence General		Shared Analytics Infrastructure Solutions shall be Xquery 1.0 standard compliant.			
SLN3	1	31	SLN3.1.31	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support relevant industry standards for electronic data exchange.	Y		
SLN3	1	32	SLN3.1.32	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support reorganization of database/index/configuration online without the need for the Solution to shut down.	Y		
SLN3	1	33	SLN3.1.33	Business Intelligence General		Shared Analytics Infrastructure Solutions shall release upgrades/patching and shall be applied with minimal loss of system availability during production hours.	Y		
SLN3	1	34	SLN3.1.34	Business Intelligence General		Solutions shall allow bulk loading to support 24/7 environments with small or no window for loading data.	Y: as agreed with State		
SLN3	1	35	SLN3.1.35	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide standards-based connectivity including Open Database Connectivity (ODBC), Java Database Connectivity (JDBC), and Web Services (WS).	Y		
SLN3	1	36	SLN3.1.36	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide scalable architecture.	Y		
SLN3	1	37	SLN3.1.37	Business Intelligence General		Shared Analytics Infrastructure Solutions shall have no limit on the size of data types, including CHAR, NUM, CLOB, BLOB and XML.	Y		
SLN3	1	38	SLN3.1.38	Business Intelligence General		Shared Analytics Infrastructure Solutions shall have no limits on the size of tables, indexes and other database-level objects.	Y: within the boudries of the agreed upon storage		
SLN3	1	39	SLN3.1.39	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support scaling across regions.	N		
SLN3	1	40	SLN3.1.40	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide flexibility in using public/private cloud version of the DBMS as an option to provide scalability in as cost effective way as needed.	Y		
SLN3	1	41	SLN3.1.41	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support native geo-spatial data types.			
SLN3	1	42	SLN3.1.42	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide Database Administration (DBA) tools for monitoring and administering DBMS and contain tools to manage the storage devices.	Y		
SLN3	1	43	SLN3.1.43	Business Intelligence General		Shared Analytics Infrastructure Solutions shall have utilities built-in to the DBMS to automate the normal day-to-day DBA operations (e.g., automated index rebuilding, free space reclamation and block reorganization).	Y		
SLN3	1	44	SLN3.1.44	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide the ability to: ' prioritize workload executions and ensure quality-of-service; ' partition indexing and aggregate management via parameters and tools; ' simulate the various workloads and mixes anticipated	Y		
SLN3	1	45	SLN3.1.45	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide workflow and collaboration support for administrator tasks.	Y		
SLN3	1	46	SLN3.1.46	Business Intelligence General		Shared Analytics Infrastructure Solutions shall run on multiple vendors' hardware and operating systems (i.e. IBM, HP, and Dell hardware, and AIX, Linux, and Windows Operating Systems)	Y		
SLN3	1	47	SLN3.1.47	Business Intelligence General		Shared Analytics Infrastructure Solutions shall make an underlying DBMS available as a data warehouse appliance so it is also available as a standalone DBMS system.	Y		
SLN3	1	48	SLN3.1.48	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support major application development interfaces (e.g. .NET interface, Java 2 Platform, Enterprise Edition [J2EE]).	Y		
SLN3	1	49	SLN3.1.49	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support various database connectivity (e.g. ODBC, JDBC).	Y		
SLN3	1	50	SLN3.1.50	Business Intelligence General		Shared Analytics Infrastructure Solutions shall have a track record with users extensively using Oracle Business Intellegence EE (OBI EE).	Y: will track users, specific soluiton TBD		
SLN3	1	51	SLN3.1.51	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support all connectivity required for the VT-selected business intelligence and extract/transform/load tools	Y'		
SLN3	1	52	SLN3.1.52	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support triggers, stored procedures and extension.	Y		
SLN3	1	53	SLN3.1.53	Business Intelligence General		The system must allow the user to export formatted reports from the system in industry standard formats, e.g., Word, Excel, PDF, OF, etc.	Y		
SLN3	1	54	SLN3.1.54	Business Intelligence General		The system must provide the ability to download and save report data to individual workstations and applications.	Y		
SLN3	1	55	SLN3.1.55	Business Intelligence General		The system must provide the ability to limit report views based on user security / access rights.	Y		
SLN3	1	56	SLN3.1.56	Business Intelligence General		The system must provide the ability to notify and distribute reports based on user specified criteria.	Y		
SLN3	1	57	SLN3.1.57	Business Intelligence General		The system must provide the ability to organize reports into a shared list (library).	Y		
SLN3	1	58	SLN3.1.58	Business Intelligence General		The system must provide the ability to present data in graphical or chart format.	Y		
SLN3	1	59	SLN3.1.59	Business Intelligence General		The system must provide the ability to roll-up (summarize data) and drill-down (view details) in reports online.	Y		
SLN3	1	60	SLN3.1.60	Business Intelligence General		The system must provide the ability to schedule the generation of reports at specific times.	Y		
SLN3	1	61	SLN3.1.61	Business Intelligence General		The system must provide the ability to sort data within reports in multiple ways.	Y		
SLN3	1	62	SLN3.1.62	Business Intelligence General		The system must provide the ability to transmit reports to various designated recipients in a secure manner.	Y		

SLN3	1	63	SLN3.1.63	Business Intelligence General		The system must restrict access to the shared list (library) or items within a shared list (library) to designated users.	Y		
SLN3	1	64	SLN3.1.64	Business Intelligence General		The system shall generate ad-hoc and standard reports in real time as well as historical for incoming and outgoing contacts.	Y		
SLN3	1	65	SLN3.1.65	Business Intelligence General		The system shall have the ability to collect data and generate periodic reports as required by the Affordable Care Act.	Y		
SLN3	1	66	SLN3.1.66	Business Intelligence General		The system shall have the ability to develop and implement reports, dashboards, scorecards, predictive analytics, what-if analysis and statistical analysis.	Y		
SLN3	1	67	SLN3.1.67	Business Intelligence General		The system shall have the ability to generate reports necessary for the Health Insurance Exchange Entities, State and Federal officials, employers and other entities, such as insurance carriers.	Y		
SLN3	1	68	SLN3.1.68	Business Intelligence General		The system shall have the ability to Provide access to standardized reporting, ad hoc queries, and data visualization.	Y		
SLN3	1	69	SLN3.1.69	Business Intelligence General		The system shall have the ability to provide reports to users in online and offline formats, such as web, fax, and paper.	Y		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Master Data Management and Integration

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN4	1	1	SLN4.1.1	MDM General	State-assigned standard identifiers	Solutions shall utilize state-assigned/identified identifiers for entities			
SLN4	1	2	SLN4.1.2	MDM General	Federal Interoperability	The Health Insurance Exchange IT systems must interact with HHS and/or other Federal agencies and data sources in order to verify and acquire data as needed through the Federal Data Service Hub.			
SLN4	1	3	SLN4.1.3	MDM General		The Solution shall apply mailing address validations including address, zip code, etc. (e.g. USPS, Pitney Bowes etc.)			
SLN4	1	4	SLN4.1.4	MDM General		The Solution shall provide the capability to link client records that are found to be duplicated or delink client records that are not duplicates			
SLN4	1	5	SLN4.1.5	MDM General		Enforce size requirements on messages as defined by the standards.			
SLN4	1	6	SLN4.1.6	MDM IdM Integration	MDM IdM Integration	MDM technology components shall rely on the central IdM technology components for authentication/authorization			
SLN4	1	7	SLN4.1.7	MDM General		Ability to migrate contact/address info from Access system into new Exchange database. Such interaction should leverage the MDM infrastructure.			
SLN4	1	8	SLN4.1.8	MDM General		Ability to verify SS# through interface with Federal data source through VT HUB/CMS HUB			
SLN4	1	9	SLN4.1.9	MDM General		A data migration strategy for existing public plan enrollees shall be developed for open enrollment in 2013 if coverage is intended to be continuous.			
SLN4	1	10	SLN4.1.10	MDM & Integration		Healthcare-related solutions will use the National Information Exchange Model (NIEM) guidelines to develop, disseminate and support standards and processes that enable the consistent, efficient and transparent exchange of data elements between programs and States.			
SLN4	1	11	SLN4.1.11	MDM & Integration		Solutions will define a set of common data elements and leverage state and agency-wide information models			
SLN4	1	12	SLN4.1.12	MDM & Integration		Solutions will have the capability to follow a scheduled data purging process in accordance with an agreed upon purge criteria.			
SLN4	1	13	SLN4.1.13	MDM & Integration		Solutions will utilize Master Data Management functions to source data for key subject areas			
SLN4	1	14	SLN4.1.14	MDM & Integration		The solution shall provide real-time interfaces to transfer data between the Exchange's solution and existing state systems (such as the Eligibility Rules Engine, state Medicaid systems, Case Management systems, Identity Access Management systems, SERFF, HIOS, Federal Data Services Hub, etc.), external systems, databases and financial systems			
SLN4		15				Vendor will develop the necessary interfaces, using the ESB, with the Federal and State Agencies as necessary to comply with ACA requirements.			
SLN4	1	16	SLN4.1.16	MDM & Integration		The solution shall provide new and or update existing two-way, real-time interfaces to transfer data between the system and 3rd party vendors (i.e. Insurance Division, insurance carriers, federal databases, etc)			
SLN4	1	17	SLN4.1.17	MDM & Integration		The solution shall provide interfaces to existing State systems that leverage existing interface designs to incorporate extensible markup language (XML) to support the requirements of the solution and associated applications.			
SLN4	1	18	SLN4.1.18	MDM & Integration		The solution shall provide functionality that knows how, and when, to communicate with interfacing systems.			
SLN4	1	19	SLN4.1.19	MDM & Integration		Provide flexibility to interface using industry standard protocols (e.g. XML, 5010, etc.)			
SLN4	1	20	SLN4.1.20	MDM & Integration		Solutions shall have the ability to convert message formats and translate coded data within messages.			
SLN4	1	21	SLN4.1.21	MDM & Integration		Solutions shall comply with all relevant HIPAA standards, including national standards for electronic health care transactions and code sets, unique employee and provider identifiers, and security and privacy of individually identifiable health information (called protected health information or PHI).			
SLN4	1	22	SLN4.1.22	MDM & Integration		Solutions shall provide support for a metadata repository for data and message conversion and transformations.			
SLN4	1	23	SLN4.1.23	MDM & Integration		Healthcare-related solutions shall at a minimum support the following standards: - Integrating the Health Enterprise (IHE): Cross-Enterprise Document Sharing (XDS, XDS.b); Cross-Community Access (XCA) - Health Level Seven (HL7) Continuity of Care Document (CCD) C32 profile - AHS ONC Direct Project			
SLN4	1	24	SLN4.1.24	MDM & Integration		Solutions shall provide the technology to implement processing logic that can manipulate data values, and the representation of those values for transport or conversion purposes. This processing logic is used to establish a common meaning of data, improve data quality or federate data from multiple sources.			
SLN4	1	25	SLN4.1.25	MDM & Integration		Solutions shall provide tooling for data source connectivity: Adapters for a range of source types beyond Relational Database Management Solutions (RDBMS's) and legacy databases (access to data stored in non-relational structures - for example, VSAM files and IMS databases), including packaged applications and Web services, the ability to access semi-structured and unstructured data (such as e-mail, websites, office productivity tools, content repositories and rich media)and the ability to interpret (as a source) XML structures			
SLN4	1	26	SLN4.1.26	MDM & Integration		Solutions shall provide tooling to support the Extract-Transform-Load (ETL) process that involves: ' Extracting data from data sources. ' Transforming it to fit business needs (which can include quality levels). ' Loading it into the target data store. ' Caching: The ability to cache federation results and various subsets of the source data to improve performance in situations where source data volumes are large; therefore, retrieving all data required for integration directly from the source is not feasible.			

SLN4	1	27	SLN4.1.27	MDM & Integration		Solutions shall have the ability to load data in a variety of approaches including (but not limited to) the following: - Bulk data extraction and loading - Granular trickle-feed acquisition and delivery - Changed-data capture (ability to identify and extract modified data) - Event-based acquisition (time-based or data-value-based)			
SLN4	1	28	SLN4.1.28	MDM & Integration		Solutions shall include the following types of transformation: - Simple transformations such as data-type conversions, string manipulations and Simple calculations - Moderate-complexity transformations, such as lookup and replace operations, aggregations, summarizations, deterministic matching and management of slowly changing dimensions - Higher-order transformations, such as sophisticated parsing operations on free-form text and rich media Facilities for developing custom transformations and extending packaged transformations - Facilities for developing custom transformations and extending packaged			
SLN4	1	29	SLN4.1.29	MDM & Integration		Solutions shall provide tooling that enables the recording (storage) or retrieving (reading) of information (data) from data stores. An example is distributed query functionality that parses incoming queries into subqueries and the execution of those subqueries, via the connectivity layer, against the respective sources where the desired data resides.			
SLN4	1	30	SLN4.1.30	MDM & Integration		Solutions shall have the capability to support the global identification, linking and/or synchronization of client and provider information across heterogeneous data sources through semantic reconciliation of master client and master provider data.			
SLN4	1	31	SLN4.1.31	MDM & Integration		The solution's data model must be expressed using commonly accepted logical data model conventions with associated metadata.			
SLN4	1	32	SLN4.1.32	MDM & Integration		Solutions shall have strong facilities, in batch and real-time mode, for profiling, cleansing, matching, linking, identifying and semantically reconciling master client and master provider data in different data sources to create and maintain golden records.			
SLN4	1	33	SLN4.1.33	MDM & Integration		The solution's business rules and associated metadata related to data cleansing shall be sufficiently visible to satisfy any audit requirements.			
SLN4	1	34	SLN4.1.34	MDM & Integration		Solutions shall include the ability to review data quality metrics and track corrective actions.			
SLN4	1	35	SLN4.1.35	MDM & Integration		Solutions shall provide dynamically configurable rules for comparing and reconciling semantics across data sources, matching (both probabilistic and tunable) across changing demographic data structures, linking data, and managing the merging and unmerging of client and provider records with full auditability and survivability.			
SLN4	1	36	SLN4.1.36	MDM & Integration		Solutions shall load data in a fast, efficient and accurate manner including data from external sources where it is matched by a proxy and not the actual client or provider ID.			
SLN4	1	37	SLN4.1.37	MDM & Integration		Solutions shall include integration middleware, including publish and subscribe mechanisms, to provide a communication backbone for the bidirectional flow of client and provider data between the central repository and the spoke solutions, be they copies or subsets of the repository, or remote applications.			
SLN4	1	38	SLN4.1.38	MDM & Integration		Solutions shall be able to leverage a range of middleware products to data sources, including all Vermont and trading partner data sources, and expose Healthcare industry-standard interfaces.			
SLN4	1	39	SLN4.1.39	MDM & Integration		Solutions shall support integration with different latency characteristics and styles (e.g. real-time, batch).			
SLN4	1	40	SLN4.1.40	MDM & Integration		Solutions shall support integration with downstream Business Intelligence (BI) and analytical requirements.			
SLN4	1	41	SLN4.1.41	MDM & Integration		Solutions shall create and manage a central, database-based Solution or index of record for master client (i.e. Master Client Index (MCI)) and master provider (i.e. Master Provider Index (MPI)) data.			
SLN4	1	42	SLN4.1.42	MDM & Integration		To support how business users collaborate in the authoring and management of client and provider data, Solutions shall provide a flexible and comprehensive workflow-based capability that can be used to create and maintain workflows supporting client and provider data maintenance across the multiple source Solutions.			
SLN4	1	43	SLN4.1.43	MDM & Integration		Solutions shall include facilities for management and controlled access to client and provider data in the MDM such as reporting on MDM activities.			
SLN4	1	44	SLN4.1.44	MDM & Integration		Solutions shall have the ability to integrate the data within the MDM with management and security tools.			
SLN4	1	45	SLN4.1.45	MDM & Integration		Solutions shall manage the policies and rules associated with solutions's privacy access rights.			
SLN4	1	46	SLN4.1.46	MDM & Integration		Solutions shall configure and manage different rules of visibility, providing different views for different roles.			
SLN4	1	47	SLN4.1.47	MDM & Integration		Solutions shall provide analytics and performance measures related to a range of processes and activities taking place within MDM, from the running of batch data loads to the execution of workflows against benchmarks to the data quality of active client data in the MDM.			
SLN4	1	48	SLN4.1.48	MDM & Integration		Solutions shall include status and management tools for the chief data steward to monitor to-do lists of users to ensure effective action takes place across the management of the master client and master provider data.			
SLN4	1	49	SLN4.1.49	MDM & Integration		Solutions shall include solution-wide meta models to help identify what users, roles, applications and solutions are responsible for which client and provider data.			
SLN4	1	50	SLN4.1.50	MDM & Integration		Solutions shall provide workflow services for remediation of quality issues in client and provider data.			
SLN4	1	51	SLN4.1.51	MDM & Integration		Solutions shall include business rules services to interrogate which rules are used by MDM by frequency and preference and to provide suggested enhancements to such business rules.			
SLN4	1	52	SLN4.1.52	MDM & Integration		Solutions shall enable the delivery of a single client and a single provider view for all stakeholders.			
SLN4	1	53	SLN4.1.53	MDM & Integration		Solutions shall be based on up-to-date, mainstream technologies, and capable of flexible and effective integration with a wide range of other application and infrastructure platform components (whether from the same vendor or not) that will be deployed by Vermont.			
SLN4	1	54	SLN4.1.54	MDM & Integration		Solutions shall protect and complement the data layer with a layer of business services for accessing and manipulating the client and provider data that is built for an SOA environment, and exposing web services interfaces.			

SLN4	1	55	SLN4.1.55	MDM & Integration		Solutions shall be capable of flexible configuration into a range of architectural styles in terms of instantiation, latency and use of client and provider data to enable different deployment scenarios, such as the consolidation, registry, coexistence and centralized scenarios.			
SLN4	1	56	SLN4.1.56	MDM & Integration		Solutions shall support ongoing client and provider data stewardship and governance requirements through monitoring of policy decisions and corrective action.			
SLN4	1	57	SLN4.1.57	MDM & Integration		Solutions shall track and maintain detailed records on all changes via interfaces and authoring to support audit requirements.			
SLN4	1	58	SLN4.1.58	MDM & Integration		The Solution must include a flexible data model that can model the complex relationships between the internal application sources inside Vermont, its trading partners, clients and providers, as well as intermediaries and other parties, with the ability to handle complex hierarchies.			
SLN4	1	59	SLN4.1.59	MDM & Integration		The solution's data model must be capable of handling at least the following categories of elements for clients and providers: - Identification - Demographics - Contact information - Relationships with other entities / providers - Interactions with other entities / providers			
SLN4	1	60	SLN4.1.60	MDM & Integration		Solutions shall include a data modeling capability that will be configurable, customizable, extensible, and upgradable.			
SLN4	1	61	SLN4.1.61	MDM & Integration		The solution's data model must be able to support Vermont standards for data content and coding where they exist.			
SLN4	1	62	SLN4.1.62	MDM & Integration		Solutions shall provide a Service Oriented Architecture based infrastructure (i.e. hub and spoke) for connecting to other solutions using an Enterprise Service Bus infrastructure.			
SLN4	1	63	SLN4.1.63	MDM & Integration		Solutions shall provide the capability to perform source to destination file integrity checks for exchange data and alert appropriate parties with issues			
SLN4	1	64	SLN4.1.64	MDM & Integration		Solutions shall build in contingencies for the storage of transactions where there is dependency on availability of data from business partners that provide authoritative data (e.g., the IRS, DHS, and SSA). The Exchange requirements will include identification of data availability requirements			
SLN4	1	65	SLN4.1.65	MDM & Integration		Solutions's Interface architecture for internal A2A (Application to Application) integration shall not have a negative impact on the user experience and expectation for application performance.			
SLN4	1	66	SLN4.1.66	MDM & Integration		Solutions's interfaces shall secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective.			
SLN4	1	67	SLN4.1.67	MDM & Integration		Solutions shall be able to support Application to Application (A2A) asynchronous messaging using web services. The messaging capabilities will be able to support a wide variety of A2A patterns including, but not limited to, the following: - Data look-up and retrieval - Data look-up with services provided by other applications - Simple bulk data transfer to/from other solutions			
SLN4	1	68	SLN4.1.68	MDM & Integration		Solutions's interfaces shall continue to operate despite failure or unavailability of individual technology components such as a server platform or network connection.			
SLN4	1	69	SLN4.1.69	MDM & Integration		Solutions's interfaces must be scalable to accommodate changes in scale including changes in user population, transaction volume, throughput and geographical distribution.			
SLN4	1	70	SLN4.1.70	MDM & Integration		Solutions shall provide the capability to detect and remediate errors caused by batch processing and real time processing via user defined rules			
SLN4	1	71	SLN4.1.71	MDM & Integration		Solutions shall provide the capability to perform source to destination file integrity checks for exchange data and alert appropriate parties with issues			
SLN4	1	72	SLN4.1.72	MDM & Integration		The Exchange shall notify CMS of an Individual disenrollment			
SLN4	1	73	SLN4.1.73	MDM & Integration		The Exchange shall send a notification to CMS of an Employee enrollment in a QHP.			
SLN4	1	74	SLN4.1.74	MDM & Integration		The Exchange shall send notification to CMS of a Small Business Employee disenrollment in a QHP.			
SLN4	1	75	SLN4.1.75	MDM Load Time	MDM Load Time	The MDM solution shall perform a full data load of Vermonters from sources within 24 hours			
SLN4	1	76	SLN4.1.76	MDM EIM Usage	MDM EIM Usage	The MDM solution shall rely on application-agnostic, enterprise information models for mastered subject areas.			
SLN4	1	77	SLN4.1.77	Mastered Subject Areas	Mastered Subject Areas	The following subject areas shall be mastered within the MDM architecture: Vermonter (Person), Provider			
SLN4	1	78	SLN4.1.78	MDM through SOA	MDM through SOA	Application software shall only access mastered subject areas through authoritative SOA/ESB-based services or through an authorized batch extract. Adhoc, one-off extracts shall not be permitted.			
SLN4	1	79	SLN4.1.79	EIM Metadata Catalog	EIM Metadata Catalog	A metadata catalog shall be maintained for the enterprise information model			
SLN4	1	80	SLN4.1.80	MDM Data Deduplication	MDM Data Deduplication	Data de-duplication and cleansing shall be employed on all mastered subject areas. This includes, but is not limited to, standardization of Postal Addresseses.			
SLN4	1	81	SLN4.1.81	Application Data Cleansing and Deduplication	Application Data Cleansing and Deduplication	Data de-duplicaiton and cleansing shall be employed in all application software to minimize the entry of "dirty" data into the MDM environment or other solutions			
SLN4	1	82	SLN4.1.82	MDM Availability	MDM Availability	The MDM solution shall support 99.9% availability in order to support other application needs			
SLN4	1	83	SLN4.1.83	Data Classification	Data Classification	Data shall be classified into the following tiers: transactional, master, and analytic			
SLN4	1	84	SLN4.1.84	Data Tier Flows	Data Tier Flows	Data updates shall follow a flow from transaction to mastered to analytic purposes; updates shall not propagate from the MDM data to the transactional applications			
SLN4	1	85	SLN4.1.85	Data Stewardship	Data Stewardship	Data stewards shall be appointed for all major subject areas of the enterprise information model which includes mastered subject areas			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Interfaces

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Source	Uni-Directional Bi-Directional	Target	Requirement Fulfilled?	Notes	Evidence
SLN5	1	1	SLN5 1.1	Interface General		The HBE solution shall implement the interfaces to and from all specified systems in the SOV EA Requirements Catalog, SLN5 Interfaces per ICD tab and the submitted HBE Interface Control Document						
SLN5	1	2	SLN5 1.2	Interface General		All internal and external application interfaces shall be brokered by the Vermont Integration Hub (VIH)'s ESB and follow ESB standards						
SLN5	1	3	SLN51.3	Interface General		The HBE solution shall implement necessary interfaces to and from the Federal Data Services Hub (CMS - FDSH)						
SLN5	1	4	SLN51.4	Interface General		The HBE solution shall implement necessary interfaces to and from SERFF						
SLN5	1	5	SLN5 1.5	Interface General		The HBE solution shall implement necessary interfaces to and from an external premium processor						
SLN5	1	6	SLN5 1.6	Interface General		The HBE solution shall implement necessary interfaces to and from the existing PeopleSoft/VISION application in Vermont						
SLN5	1	7	SLN5 1.7	Interface General		The HBE solution shall implement necessary interfaces to and from an external interface to support financial management						
SLN5	1	8	SLN5 1.8	Interface General		The HBE solution shall implement necessary interfaces to and from the new Call/Customer Support Center Vendor						
SLN5	1	9	SLN5 1.9	Interface General		The HBE solution shall implement necessary interfaces to and from the SOV centralized document scanning facility						
SLN5	1	10	SLN51.10	Interface General		The HBE solution shall implement necessary interfaces to and from the SOV ACCESS system						
SLN5	1	11	SLN51.11	Physical Interface		Federal Data Services Hub Interface (CMS)	CMS	Bi-Directional	HBE			
SLN5	1	12	SLN51.12	Interface Data Flow		Report: APTC/CSR Payment	CMS	Uni-Directional	HBE			
SLN5	1	13	SLN51.13	Interface Data Flow		Report: Premium Payment History (Monthly)	HBE	Uni-Directional	CMS			
SLN5	1	14	SLN51.14	Interface Data Flow		Enrollment Data - Plan, Premium, APTC/CSR, State Premium Subsidy, State CSR, Household Contribution Amount, HIPP (Monthly)	HBE	Uni-Directional	CMS			
SLN5	1	15	SLN51.15	Interface Data Flow		Publish Carrier and Plan Information (Needed if SERFF interface is not in place)	HBE	Bi-Directional	CMS			
SLN5	1	16	SLN51.16	Interface Data Flow		Provide Plan Non-Renewal, Decertification, and Change in Availability Notices (Needed if SERFF interface is not in place)	HBE	Bi-Directional	CMS			
SLN5	1	17	SLN51.17	Interface Data Flow		Provide Rate and Benefit Data (Needed if SERFF interface is not in place)	HBE	Bi-Directional	CMS			
SLN5	1	18	SLN51.18	Interface Data Flow		HBE Notifies CMS of Individual Disenrollment from QHP	HBE	Bi-Directional	CMS			
SLN5	1	19	SLN51.19	Interface Data Flow		Validate Individual SSN	HBE	Bi-Directional	CMS			
SLN5	1	20	SLN51.20	Interface Data Flow		CMS or IRS Calculates and Returns Individual MAX APTC Request	HBE	Bi-Directional	CMS			
SLN5	1	21	SLN51.21	Interface Data Flow		Verify Lawful Presence Request, CMS Coordinates with Dept Homeland Security and SSA	HBE	Bi-Directional	CMS			
SLN5	1	22	SLN51.22	Interface Data Flow		Verify Household Income Request, CMS Coordinates with IRS	HBE	Bi-Directional	CMS			
SLN5	1	23	SLN51.23	Interface Data Flow		Initiate Citizenship Verification	HBE	Bi-Directional	CMS			
SLN5	1	24	SLN51.24	Interface Data Flow		Validate Immigration Verification	HBE	Bi-Directional	CMS			
SLN5	1	25	SLN51.25	Interface Data Flow		Send Documentation for Review to Verify Lawful Presence	HBE	Uni-Directional	CMS			
SLN5	1	26	SLN51.26	Interface Data Flow		Verify Individual Unemployment Insurance Request	HBE	Bi-Directional	CMS			
SLN5	1	27	SLN51.27	Interface Data Flow		HBE Reports Individual Exemption Status to IRS through CMS	HBE	Bi-Directional	CMS			
SLN5	1	28	SLN51.28	Interface Data Flow		Verify Employer EIN Request	HBE	Bi-Directional	CMS			
SLN5	1	29	SLN51.29	Interface Data Flow		HBE Notifies of Employer Participation in SHOP Exchange, CMS notifies IRS	HBE	Bi-Directional	CMS			
SLN5	1	30	SLN51.30	Interface Data Flow		HBE Notifies of Employer Termination from Participation in SHOP Exchange, CMS notifies IRS	HBE	Bi-Directional	CMS			
SLN5	1	31	SLN51.31	Interface Data Flow		HBE Notifies CMS of Exchange Appeal Decision, CMS notifies IRS	HBE	Bi-Directional	CMS			
SLN5	1	32	SLN51.32	Interface Data Flow		Provide Plan Quality Rating Methodology	HBE	Bi-Directional	CMS			
SLN5	1	33	SLN51.33	Interface Data Flow		Exchange Financial Statements	HBE	Uni-Directional	CMS			
SLN5	1	34	SLN51.34	Physical Interface		Premium Processor Vendor Interface	HBE	Bi-Directional	Premium Processor			
SLN5	1	35	SLN51.35	Interface Data Flow		Report: Premium Payment History (Monthly)	Premium Processor	Uni-Directional	HBE			
SLN5	1	36	SLN51.36	Interface Data Flow		Enrollment Data - Plan, Premium, APTC/CSR, State Premium Subsidy, State CSR, Household Contribution Amount, HIPP, Individual Public Premium Amount (To be used for Billing)	HBE	Uni-Directional	Premium Processor			
SLN5	1	37	SLN51.37	Interface Data Flow		Underpayment Notification	Premium Processor	Uni-Directional	HBE			
SLN5	1	38	SLN51.38	Interface Data Flow		Late Payment Notification	Premium Processor	Uni-Directional	HBE			
SLN5	1	39	SLN51.39	Interface Data Flow		Individual Public Premium Assistance Billing, Collection Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	40	SLN51.40	Interface Data Flow		APTC/CSR Payment Summaries (based on CMS Report)	Premium Processor	Uni-Directional	VISION			
SLN5	1	41	SLN51.41	Interface Data Flow		State Premium Subsidy Payment Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	42	SLN51.42	Interface Data Flow		User Fee Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	43	SLN51.43	Interface Data Flow		Issuer Payment Remittance Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	44	SLN51.44	Interface Data Flow		Individual Premium (QHP) Billing, Collection Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	45	SLN51.45	Interface Data Flow		Employer Premium (QHP) Billing, Collection Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	46	SLN51.46	Interface Data Flow		State CSR Payment Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	47	SLN51.47	Interface Data Flow		HIPP Payment Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	48	SLN51.48	Interface Data Flow		Refund Remitted Overpayment	Issuers	Uni-Directional	Premium Processor			
SLN5	1	49	SLN51.49	Interface Data Flow		Aggregate Premium Payments	HBE	Uni-Directional	Premium Processor			
SLN5	1	50	SLN51.50	Interface Data Flow		State CSR Funds	DFR	Uni-Directional	Premium Processor			
SLN5	1	51	SLN51.51	Interface Data Flow		State Premium Subsidy Funds	DFR	Uni-Directional	Premium Processor			
SLN5	1	52	SLN51.52	Interface Data Flow		Agent Commissions	Premium Processor	Uni-Directional	Agent			
SLN5	1	53	SLN51.53	Interface Data Flow		Enrollee Invoice Information (Medicaid Plans)	HBE	Uni-Directional	Premium Processor			
SLN5	1	54	SLN51.54	Physical Interface		SERFF Interface	SERFF	Bi-Directional	HBE			
SLN5	1	55	SLN51.55	Interface Data Flow		Provide Required Carrier and Plan Information	SERFF	Uni-Directional	HBE			
SLN5	1	56	SLN51.56	Interface Data Flow		Provide Rate and Benefit Data	SERFF	Uni-Directional	HBE			

SLN5	1	57	SLN51.57	Interface Data Flow		Provide Plan Non-Renewal and Change in Availability Notices	SERFF	Uni-Directional	HBE			
SLN5	1	58	SLN51.58	Interface Data Flow		Provide Response to Solicitation	SERFF	Uni-Directional	HBE			
SLN5	1	59	SLN51.59	Interface Data Flow		Provide QHP Agreement Materials	SERFF	Uni-Directional	HBE			
SLN5	1	60	SLN51.60	Interface Data Flow		Enroll, Register, Dropout, Modify, Reconcile Plan	SERFF	Uni-Directional	HBE			
SLN5	1	61	SLN51.61	Interface General		Verify Individual Incarceration Status Request	HBE	Uni-Directional	CMS			
SLN5	1	62	SLN51.62	Physical Interface		Issuer/Carrier Interface	HBE	Bi-Directional	Issuers			
SLN5	1	63	SLN51.63	Interface Data Flow		Report: Monthly Enrollment Reports for Reconciliation	HBE	Uni-Directional	Issuers			
SLN5	1	64	SLN51.64	Interface Data Flow		Report: Premium Payment History (monthly)	Premium Processor	Uni-Directional	Issuers			
SLN5	1	65	SLN51.65	Interface Data Flow		Report: Issuer Premium Remittance (less user fees) Payment Transaction Information	Premium Processor	Uni-Directional	Issuers			
SLN5	1	66	SLN51.66	Interface Data Flow		Report: APTC/CSR Payment	HBE	Uni-Directional	Issuers			
SLN5	1	67	SLN51.67	Interface Data Flow		Employer Group Setup	HBE	Uni-Directional	Issuers			
SLN5	1	68	SLN51.68	Interface Data Flow		Individual Enrollment Data - Plan, Premium, APTC/CSR, State Premium Subsidy, State CSR, Household Contribution Amount, HIPP	HBE	Bi-Directional	Issuers			
SLN5	1	69	SLN51.69	Interface Data Flow		Notification of Individual Disenrollment from QHP	HBE	Bi-Directional	Issuers			
SLN5	1	70	SLN51.70	Interface Data Flow		Notification of Renewals and Changes to Individual Enrollee	HBE	Bi-Directional	Issuers			
SLN5	1	71	SLN51.71	Interface Data Flow		Individual or Employer Premium Payments	Premium Processor	Bi-Directional	Issuers			
SLN5	1	72	SLN51.72	Interface Data Flow		CSR Funds	CMS	Uni-Directional	Issuers			
SLN5	1	73	SLN51.73	Interface Data Flow		APTC Funds	CMS	Uni-Directional	Issuers			
SLN5	1	74	SLN51.74	Interface Data Flow		Refund Remitted Overpayment	Issuers	Uni-Directional	Premium Processor			
SLN5	1	75	SLN51.75	Interface Data Flow		Underpayment Notification	Premium Processor	Uni-Directional	Issuers			
SLN5	1	76	SLN51.76	Interface Data Flow		Late Payment Notification	Premium Processor	Uni-Directional	Issuers			
SLN5	1	77	SLN51.77	Physical Interface		ACCESS System Interface (State Systems)	ACCESS	Bi-Directional	HBE			
SLN5	1	78	SLN51.78	Interface Data Flow		Process Individual Eligibility	ACCESS	Bi-Directional	HBE			
SLN5	1	79	SLN51.79	Interface Data Flow		Create, Merge, Update, Match Customer	ACCESS	Bi-Directional	HBE			
SLN5	1	80	SLN51.80	Interface Data Flow		HIPP	DFR	Uni-Directional	HBE			
SLN5	1	81	SLN51.81	Interface Data Flow		Employment Qtrly Wage Report	DOL	Uni-Directional	HBE			
SLN5	1	82	SLN51.82	Interface Data Flow		Unemployment Report	DOL	Uni-Directional	HBE			
SLN5	1	83	SLN51.83	Interface Data Flow		HIPP Amount	HBE	Uni-Directional	DCF/ESD			
SLN5	1	84	SLN51.84	Interface Data Flow		State CSR Amount	DCF/ESD	Uni-Directional	HBE			
SLN5	1	85	SLN51.85	Interface Data Flow		State Premium Subsidy Amount	DCF/ESD	Uni-Directional	HBE			
SLN5	1	86	SLN51.86	Interface Data Flow		Enroll, Register, Dropout, Modify, Reconcile Plan	HBE	Uni-Directional	ACCESS			
SLN5	1	87	SLN51.87	Interface Data Flow		Operating Expense, Salary Information	HBE	Uni-Directional	DFR			
SLN5	1	88	SLN51.88	Interface Data Flow		Head of Household Eligibility	VSHA	Uni-Directional	HBE			
SLN5	1	89	SLN51.89	Interface Data Flow		Update Individual status	VDH	Uni-Directional	HBE			
SLN5	1	90	SLN51.90	Interface General		Verify Individual State Residency Status Request	Vital Records	Uni-Directional	HBE			
SLN5	1	91	SLN51.91	Physical Interface		Siebel Interface	Siebel	Bi-Directional	ESB			
SLN5	1	92	SLN51.92	Interface Data Flow		Data Flow between OLTP and OLAP	Siebel	Uni-Directional	Informatica			
SLN5	1	93	SLN51.93	Physical Interface		OPA Interface	OPA	Bi-Directional	HBE			
SLN5	1	94	SLN51.94	Interface Data Flow		Validate Customer	OPA	Bi-Directional	HBE			
SLN5	1	95	SLN51.95	Interface Data Flow		Validate Citizenship	OPA	Bi-Directional	HBE			
SLN5	1	96	SLN51.96	Interface Data Flow		Validate Tax Record	OPA	Bi-Directional	HBE			
SLN5	1	97	SLN51.97	Interface Data Flow		Verify Individual Eligibility for MEC Request	HBE	Bi-Directional	OPA			
SLN5	1	98	SLN51.98	Interface General		Verify Individual Eligibility for Employer Sponsored MEC Request	HBE	Bi-Directional	OPA			
SLN5	1	99	SLN51.99	Interface Data Flow		Verify Individual Eligibility for other MEC for APTC and CSR Request	HBE	Bi-Directional	OPA			
SLN5	1	100	SLN51.100	Interface Data Flow		HBE Notifies Individual Potential Eligibility Other Than MAGI	HBE	Bi-Directional	OPA			
SLN5	1	101	SLN51.101	Physical Interface		OBIEE Interface	Siebel	Bi-Directional	OBIEE			
SLN5	1	102	SLN51.102	Interface Data Flow		HBE Reporting Tool	Siebel	Bi-Directional	OBIEE			
SLN5	1	103	SLN51.103	Physical Interface		MDM Interface	MDM	Bi-Directional	ESB			
SLN5	1	104	SLN51.104	Interface Data Flow		Create, Merge, Update, Match, Fetch Customer	MDM	Bi-Directional	ACCESS			
SLN5	1	105	SLN51.105	Interface Data Flow		Create, Merge, Update, Match, Fetch Customer	MDM	Bi-Directional	HBE			
SLN5	1	106	SLN51.106	Physical Interface		Informatica ETL Job Interface	Informatica	Bi-Directional	OBIEE			
SLN5	1	107	SLN51.107	Interface Data Flow		Data Flow between OLTP and OLAP	Siebel	Uni-Directional	Informatica			
SLN5	1	108	SLN51.108	Physical Interface		MMIS Interface	HBE	Uni-Directional	MMIS			
SLN5	1	109	SLN51.109	Interface Data Flow		Daily/Monthly Individual Eligibility	HBE	Uni-Directional	MMIS			
SLN5	1	110	SLN51.110	Interface Data Flow		Reconciliation Report	HBE	Uni-Directional	MMIS			
SLN5	1	111	SLN51.111	Physical Interface		Call Center Interface	CC	Bi-Directional	HBE			
SLN5	1	112	SLN51.112	Interface Data Flow		Problem Resolution	CC	Bi-Directional	HBE			
SLN5	1	113	SLN51.113	Physical Interface		Content Management Interface	CMS	Bi-Directional	HBE			
SLN5	1	114	SLN51.114	Interface Data Flow		CM Data Flow	CM	Bi-Directional	Premium Processor			
SLN5	1	115	SLN51.115	Physical Interface		KM Management Interface	KM	Bi-Directional	HBE			
SLN5	1	116	SLN51.116	Physical Interface		Scanning/Paper processing Interface	Scanning/Paper	Uni-Directional	HBE			
SLN5	1	117	SLN51.117	Physical Interface		People Soft Interface	People Soft	Bi-Directional	HBE			
SLN5	1	118	SLN51.118	Physical Interface		SOA/ESB Interface	ESB	Bi-Directional	HBE			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM) MITA									
Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN6	1	1	SLN6.1.1	Modularity		[Solutions shall] Uses a modular, flexible approach to systems development, including the use of open interfaces and exposed Application Programming Interfaces (API); the separation of standardized business rule definitions from core programming; and the availability of standardized business rule definitions in both human and machine- readable formats. The States commit to formal system development methodology and open, reusable system architecture.			
SLN6	1	2	SLN6.1.2	MITA		States [shall] align to and advance increasingly in MITA maturity for business, architecture, and data by Conducting MITA Self Assessments, Developing MITA Roadmaps, Developing Concept of Operations (COO), and Business Process Models (BPM)			
SLN6	1	3	SLN6.1.3	Industry Standards		[Solutions shall] Ensures alignment with, and incorporation of, industry standards: the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security, privacy and transaction standards; accessibility standards established under section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities, and compliance with Federal Civil Rights laws; standards adopted by the Secretary under section 1104 of the Affordable Care Act; and standards and protocols adopted by the Secretary under section 1561 of the Affordable Care Act. Activity includes the following: Identification of industry standards and Incorporation of industry standards in requirements, development, and testing phases			
SLN6	1	4	SLN6.1.4	Leverage		State solutions should promote sharing, leverage, and reuse of Medicaid technologies and systems within and among States. Activity includes the following: Multi-state efforts, Availability for reuse, Identification of open source, cloud-based, and commercial products, Customization, and Transition and retirement plans			
SLN6	1	5	SLN6.1.5	Business Results		Systems should support accurate and timely processing of claims (including claims of eligibility), adjudications, and effective communications with providers, beneficiaries, and the public. Activity includes the following: Degree of automation, Customer Service, Performance standards and testing			
SLN6	1	6	SLN6.1.6	Reporting		Solutions should produce transaction data, reports, and performance information that contributes to program evaluation, continuous improvement in business operations, transparency, and accountability. Activity includes the following: Accurate data, Interfaces with designated federal repositories or hubs, Automatic generation of reports, Audit trails			
SLN6	1	7	SLN6.1.7	Interoperability		Systems must ensure seamless coordination and integration with the Exchanges (whether run by the state or federal government), and allow interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services. Interactions with the Exchange, Interactions with other entities			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Rules

Base	Level	Sub.	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN7	1	1	SLN7.1.1	Rules		Solutions shall support data verification and consistency checks.			
SLN7	1	2	SLN7.1.2	Rules		Solutions shall support seamless and easy user interaction			
SLN7	1	3	SLN7.1.3	Rules		Solutions shall provide context sensitive help and extensive documentation			
SLN7	1	4	SLN7.1.4	Rules		The Rules Engine must be able to submit business rules to a federal repository at such time as the repository exists.			
SLN7	1	5	SLN7.1.5	Rules		Solutions shall support high performance and scalability, including the following characteristics: - High performance for large rule bases (more than 20,000 rules) - Ability to share rule sets across multiple engines - Dynamic and static execution versions for performance - Multiple, cross-platform support - Segmented repositories - Pre-built rule paths - Rule pre-fetch to memory - Parallel rule search - Ability to compile rule sequences into base languages like C++, Java and C#			
SLN7	1	6	SLN7.1.6	Rules		Solutions shall support advanced inference features, including: - Truth maintenance to support parallel rule execution - Inductive and deductive problem sets supported - Recursive rules supported - Rule aggregation supported - Links to simulation capabilities - Agent or daemon links - Object inheritance supported - Multiple-engine support			
SLN7	1	7	SLN7.1.7	Rules		Solutions shall include rule management features for the execution engine, including: - Rule extensibility - Rule mapping to owners and stewards - Rule change impact analysis purposes - Integration/coordination of distributed rule engines with a corporate master - Ability to rerun the engine for a point which has passed (for example, after 1 January, still able to rerun year-end jobs with 31 December rules) - Ability to enter new rules or changes to become effective on a future date (for example, ability to put in the rule changes for 1 January in December) - Rule consistency/collision checks - Rule versioning - Release versioning and rollback - Rule security			
SLN7	1	8	SLN7.1.8	Rules		Solutions shall include a rule repository for global rule management, including: - nomadic support - an extensible meta model - rule merge support - versioning/lockout - rule promotion - change management - electronic rule distribution (publish or subscribe) - security			
SLN7	1	9	SLN7.1.9	Rules		Solutions shall support ease of use in operation/development and administration, including: i. Rule-firing audit report capabilities ii. Rule views by project or role iii. Ability to be used as a wizard/plug-in for multiple development environments iv. Dynamic rule change supported v. Rules separated from the engine vi. Constraints naturally supported			
SLN7	1	10	SLN7.1.10	Rules		Solutions shall provide the capability to associate effective dates with each program and rule in the rules engine.			
SLN7	1	11	SLN7.1.11	Rules		Solutions shall support Compute values based on input data			
SLN7	1	12	SLN7.1.12	Rules		Solutions shall provide the capability to associate a rule with multiple program profiles.			
SLN7	1	13	SLN7.1.13	Rules		Solutions shall provide the capability to identify and apply a rule change appropriately to existing cases.			
SLN7	1	14	SLN7.1.14	Rules		Solutions shall provide the capability to copy an existing rule to create a new rule.			
SLN7	1	15	SLN7.1.15	Rules		Solutions shall provide the ability to identify all other rules that are dependent on a specific rule by allowing rules association			
SLN7	1	16	SLN7.1.16	Rules		Solutions shall provide the capability to generate and display a flow chart of each program profile.			
SLN7	1	17	SLN7.1.17	Rules		Solutions shall provide the ability to maintain and display the history of each rule change in the rules engine.			
SLN7	1	18	SLN7.1.18	Rules		Solutions shall provide the capability to add additional table-driven variables to support new regulations using a rules engine.			
SLN7	1	19	SLN7.1.19	Rules		Solutions shall include an automated rule build capability for rule repository propagation through the environments Development, Integration/Test, User Acceptance Testing and Production.			
SLN7	1	20	SLN7.1.20	Rules		Solutions shall support the selection of business process path			
SLN7	1	21	SLN7.1.21	Rules		Solutions shall have the ability to expose sets of interrelated rules in the rules repository as either a web service and/or in a interactive, web-based interview format.			
SLN7	1	22	SLN7.1.22	Rules		Solutions shall have the ability to create customizable web-based, interview sessions based on defined rule sets.			
SLN7	1	23	SLN7.1.23	Rules		The Solution must facilitate the creation and maintenance of rules referencing complex data relationships this will include, but not be limited to, rules referencing complex many-to-many relationships between entity types			
SLN7	1	24	SLN7.1.24	Rules		The Solution must have the ability for text documentation and meta-data to be included as part of the rules repository.			
SLN7	1	25	SLN7.1.25	Rules		The Solution will have documentation for assisting rule authors and administrators with best practices for rule repository creation and maintenance, repository check-in/checkout, repository promotion across environments.			
SLN7	1	26	SLN7.1.26	Rules		The Vendor shall partner with the AHS management and Rule Author(s) to design suitable policy models for Eligibility Determination and other rules to be automated using the proposed Rules Management System.			
SLN7	1	27	SLN7.1.27	Rules		The Vendor shall transform all of the state's health-benefit program rules into a format that can be consumed by the proposed Rules Management System.			

SLN7	1	28	SLN7.1.28	Rules		The Vendor shall assist the State with creating a process and systems capability that posts formal rules to the web for general review by the public.			
SLN7	1	29	SLN7.1.29	Rules		The Vendor shall create the program rules in the proposed Rules Management System and test them in an established environment.			
SLN7	1	30	SLN7.1.30	Rules		The Vendor shall create a valid set of rules to transition from the current mainframe system to the proposed Rules Management system in preparation for the new SOA system.			
SLN7	1	31	SLN7.1.31	Rules		The Vendor rules management team will work with and Mentor the State staff Rule Author(s) in the best practices of: - Converting rules from federal or legislative documents into properly structured rules that can be consumed by the proposed Rules Management System and writing future rules in such a way that eases the transition - Capturing meta-data about each of the rules sets and how they function			
SLN7	1	32	SLN7.1.32	Rules		The Vendor shall provide guidance on: - How best to store and look up the meta-data - Defining the Lifecycle of rule sets - How to integrate or flow rules - How to provide help or commentary on rules - General use of the proposed Rules Management System			
SLN7	1	33	SLN7.1.33	Rules		The Vendor shall provide selected State staff with holistic education on the proposed Rules Management system that includes (but is not limited to): - Knowledge about how the proposed Rules Management system works - Knowledge about how to structure the Rule Author(s) to meet the Agency goals - Knowledge about how to create, maintain and update rules in the proposed Rules Management system			
SLN7	1	34	SLN7.1.34	Rules		Solutions shall support mechanisms and ease of use for users to edit rules while maintaining compliance with CMS rules.			
SLN7	1	35	SLN7.1.35	Rules		The Vendor must follow all standards defined by CMS in Guidance for Exchange and Medicaid Technology Systems and Enhanced Funding Requirements: Seven Conditions and Standards; and other federal guidelines yet to be defined; including use a technology neutral rules repository.			
SLN7	1	36	SLN7.1.36	Rules		Solutions shall support design for a multi-step decision			
SLN7	1	37	SLN7.1.37	Rules		Solutions shall have the ability to tune individual steps in the overall decision process for maximum performance by the execution engine			
SLN7	1	38	SLN7.1.38	Rules		Solutions shall support reporting requirements either natively or integrate with other reporting tools to provide reporting			
SLN7	1	39	SLN7.1.39	Rules		Solutions shall support repository infrastructure for rule storage and versioning			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Portal

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Req Notes	Requirement Fulfilled?	Evidence
SLN8	1	1	SLN8.1.1			Solutions shall provide a portal UI framework that separates content from logic and is robust, scalable and interoperable with W3C Web-based standards.			
SLN8	1	2	SLN8.1.2			Solutions shall provide content metadata attributes for portal extensibility.			
SLN8	1	3	SLN8.1.3			Solutions shall provide multimedia Web content management capabilities.			
SLN8	1	4	SLN8.1.4			Solutions shall provide wiki- and blog-based capabilities			
SLN8	1	5	SLN8.1.5			Solutions shall provide XHTML e-form capabilities.			
SLN8	1	6	SLN8.1.6			Solutions shall provide survey engine capabilities.			
SLN8	1	7	SLN8.1.7			Solutions shall provide chat and instant messaging (IM) support.			
SLN8	1	8	SLN8.1.8			Solutions shall provide the capability to consume externally available mapping Web services.			
SLN8	1	9	SLN8.1.9			Solutions shall provide portlet capabilities.			
SLN8	1	10	SLN8.1.10			Solutions shall provide inter-portlet communications that are robust, scalable and reliable.			
SLN8	1	11	SLN8.1.11			Solutions shall provide search engine capabilities.			
SLN8	1	12	SLN8.1.12			Solutions shall provide session management capabilities to support user sessions and coordinated back-end application functionality.			
SLN8	1	13	SLN8.1.13			Solutions shall provide taxonomy-based cataloging of portal resources.			
SLN8	1	14	SLN8.1.14			Solutions shall provide index-based search capabilities.			
SLN8	1	15	SLN8.1.15			The Solution must allow for user analytics to be captured and reported			
SLN8	1	16	SLN8.1.16			Solutions shall provide support for multiple languages and character set encoding standards.			
SLN8	1	17	SLN8.1.17			Solutions shall provide portal personalization and customization capabilities for the constituent user experience.			
SLN8	1	18	SLN8.1.18			Solutions shall support access from multiple channels and devices.			
SLN8	1	19	SLN8.1.19			Solutions shall provide support for Web content management solution that is robust and scalable.			
SLN8	1	20	SLN8.1.20			Solutions shall provide time-based content expiration and version management capabilities.			
SLN8	1	21	SLN8.1.21			Solutions shall provide Web content management workflow management.			
SLN8	1	22	SLN8.1.22			Solutions shall provide syndicated content capabilities including creation and subscription to RSS feeds			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
ECM

Base	Level	Sub	Req ID New	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN9	1	1	SLN9.1.1			Solutions shall provide the ability to capture solution-generated documents and store them at appropriate level (e.g. individual, case, program, application, various workflow/process)			
SLN9	1	2	SLN9.1.2			Solutions shall ensure version control of documents as they are changed or modified			
SLN9	1	3	SLN9.1.3			Solutions shall allow rollback to a previous version of a document			
SLN9	1	4	SLN9.1.4			Solutions shall enable collaborative document creation and/or markup			
SLN9	1	5	SLN9.1.5			Solutions shall enable attachment of documents to e-mails and e-mail distribution lists			
SLN9	1	6	SLN9.1.6			Solutions shall utilize the solutions authorization and access control for file level security			
SLN9	1	7	SLN9.1.7			Solutions shall have the ability to, based on rules or context, automate the creation of indexing, meta data and overall taxonomy			
SLN9	1	8	SLN9.1.8			Solutions shall have robust bulk load and conversion features			
SLN9	1	9	SLN9.1.9			Solutions shall provide the capability to communicate natively with the document management API			
SLN9	1	10	SLN9.1.10			Solutions shall provide the capability to access the output of the document management system over the Internet and/or Intranet web sites.			
SLN9	1	11	SLN9.1.11			Solutions shall develop a user guide that can be accessed online and printed on demand.			
SLN9	1	12	SLN9.1.12			Solutions shall provide the ability to store electronic forms (solution generated or 3rd-party generated forms)			
SLN9	1	13	SLN9.1.13			Solutions shall provide the capability for online access to policy and procedure and training materials.			
SLN9	1	14	SLN9.1.14			Solutions shall be integrated with document processing center workflow.			
SLN9	1	15	SLN9.1.15			Solutions shall provide scanning software that is configurable to accommodate user-defined field edits such as the exclusion or inclusion of special characters.			
SLN9	1	16	SLN9.1.16			Solutions shall accommodate multiple imaging locations.			
SLN9	1	17	SLN9.1.17			Solutions shall integrate the Imaging and Document Management System with VT HSE Platform.			
SLN9	1	18	SLN9.1.18			Solutions shall provide the capability to access VT HSE Platform to extract data to pre-populate index fields, and/or values on forms.			
SLN9	1	19	SLN9.1.19			Solutions shall provide the capability to send and receive faxed and e-form documents, process the data and image directly into and out of the system including the ability to automatically send confirmation of transmission to the			
SLN9	1	20	SLN9.1.20			Solutions shall provide the capability for performing conditional routing that will send documents to a specific queue or inbox, either manually or electronically, based on preset conditions as defined by the User.			
SLN9	1	21	SLN9.1.21			Solutions shall provide the capability to store and view a multiple page document as a single document.			
SLN9	1	22	SLN9.1.22			Solutions shall provide the capability to attach notes, annotations, e-mails and other documents to an original scanned document at any time without rescanning.			
SLN9	1	23	SLN9.1.23			Solutions shall provide the capability to scan and store imaged documents and electronic files			
SLN9	1	24	SLN9.1.24			Solutions shall provide the capability to notify the user when a duplicate document has been received so the user can decide whether to use the previously received document, replace the existing document or store the new document			
SLN9	1	25	SLN9.1.25			Solutions shall provide the capability to link imaged documentation together and link it to an individual and/or cases within VT HSE Platform.			
SLN9	1	26	SLN9.1.26			Solutions shall provide the capability to record user and workstation identification for each document processed, accessed or updated.			
SLN9	1	27	SLN9.1.27			Solutions shall provide the capability for documents to be grouped together during scanning based on user defined criteria.			
SLN9	1	28	SLN9.1.28			Solutions shall provide the capability to allow the User to manually remove, rescan and replace a previously scanned image or document(s).			

SLN9	1	29	SLN9.1.29			Solutions shall provide the capability to employ user-defined form/template, indexes and/or field values for recognition and retrieval of documents.			
SLN9	1	30	SLN9.1.30			Solutions shall provide the capability to validate data captured from specific fields on forms electronically read by OCR/OMR/ICR.			
SLN9	1	31	SLN9.1.31			Solutions shall provide the capability for archived documents to be retrieved and re-indexed.			
SLN9	1	32	SLN9.1.32			Solutions shall provide the capability to permanently delete documents based on user defined criteria.			
SLN9	1	33	SLN9.1.33			Solutions shall provide the capability to interface with other imaging systems using industry standard interfaces and file formats.			
SLN9	1	34	SLN9.1.34			Solutions shall enable indexing and searching of documents by a variety of user-defined metadata attributes			
SLN9	1	35	SLN9.1.35			Solutions shall provide the capability to version multiple copies of scanned documents.			
SLN9	1	36	SLN9.1.36			Solutions shall provide the capability to scan at least 80 pages per minute.			
SLN9	1	37	SLN9.1.37			Solutions shall provide image retrieval response times within a minimum of two seconds for all documents stored in the system.			
SLN9	1	38	SLN9.1.38			Solutions shall provide the capability for simplex and duplex scanning.			
SLN9	1	39	SLN9.1.39			Solutions shall provide an imaging solution that includes advanced Optical Character Recognition, Intelligent Character Recognition, and Optical Mark Recognition capabilities with a minimum 90% accuracy rate and the ability to regulate the			
SLN9	1	40	SLN9.1.40			Solutions shall provide audit trail functions with the ability to log every step in the process to a database for query and reporting purposes.			
SLN9	1	41	SLN9.1.41			Solutions shall automatically calculate transfer and destruction dates (and assign records ready for deletion to the appropriate review process for approval of final deletion) for all records in the retention schedules.			
SLN9	1	42	SLN9.1.42			Solutions shall provide email notification of disposition results			
SLN9	1	43	SLN9.1.43			Solutions shall include a workflow tool to support the records management process			
SLN9	1	44	SLN9.1.44			Solutions shall provide support for full text search			
SLN9	1	45	SLN9.1.45			Solutions shall allow users to manually or automatically classify records or classified automatically based on a policy/rules engine			
SLN9	1	46	SLN9.1.46			Solutions shall allow administrators and authorized users to create, apply, view or remove legal holds for individual or multiple records			
SLN9	1	47	SLN9.1.47			Solutions shall enable declaration of email: • From Microsoft Outlook as records using drag-and-drop or menu functions • As it is inbound to and outbound from the email system • In Microsoft Outlook journal folders			
SLN9	1	48	SLN9.1.48			Solutions shall have the capability to produce colored and bar-coded labels created for physical records			
SLN9	1	49	SLN9.1.49			Solutions shall have the capability to check records in and out using barcodes, with adherence to security permissions and support the use of barcode scanners for the purpose			
SLN9	1	50	SLN9.1.50			Solutions shall have the capability to track all types and sizes of storage containers within storage locations			
SLN9	1	51	SLN9.1.51			Solutions shall be compliant with U.S. Department of Defense 5015.2-STD Electronic Records Management Standard			
SLN9	1	52	SLN9.1.52			Solutions shall have the ability for an administrator to create and maintain retention schedules			
SLN9	1	53	SLN9.1.53			Solutions shall have the ability to create disposition, legal hold and audit reports for the records			

SLN9	1	54	SLN9.1.54			Solutions shall provide content authoring capabilities including: • Provide a structured container for the content (e.g. document) • Support reuse via Copy and Paste or "Save As" • Tracking of changes to content within a container • Drag-and-drop page layout • Ability for collaboration by allowing the "single control" to transfer between authors, reviewers and authorizers • Real-time active collaboration allowing multiple authors to review and update the content in a container during the course of a shared session • Standard templates to make authoring documents within certain parameters • Facilitate the use of Microsoft Office creation tools to submit content directly into the WCM repository • The bulk import and export of XML content for integration and migration • Reuse of content and templates to enforce a common "look and feel" and brand identity • A flexible and extensible workflow to manage authoring review and approval of content across its life cycle • The ability to expire and retire content.			
SLN9	1	55	SLN9.1.55			Solutions shall provide built-in viewers/converters for a wide variety of file types			
SLN9	1	56	SLN9.1.56			Solutions shall support the combination of text and other page elements, such as graphics, logos and buttons and multimedia, such as audio/video and Flash.			
SLN9	1	57	SLN9.1.57			Solutions shall include the ability to support content in multiple languages			
SLN9	1	58	SLN9.1.58			Solutions shall support multiple versions of the same site using the same WCM instance and repository			
SLN9	1	59	SLN9.1.59			Solutions shall display content targeted toward specific user profiles			
SLN9	1	60	SLN9.1.60			Solutions shall target content based on visitor-supplied preferences			
SLN9	1	61	SLN9.1.61			Solutions shall personalize a site based on customer transaction data, apply personalization rules to elements smaller than pages and use perceived behavior employing mechanisms to assess the behavior of an individual user (known or unknown) in real time and enable choice of delivered content based on that analysis)			
SLN9	1	62	SLN9.1.62			Solutions shall provide reporting of • The status and history of a piece of content			
SLN9	1	63	SLN9.1.63			Solutions shall provide out-of-the-box log file analysis			
SLN9	1	64	SLN9.1.64			Solutions shall have the ability to find broken links and repair them			
SLN9	1	65	SLN9.1.65			Solutions shall the capability to track and report on-site use and demographics			
SLN9	1	66	SLN9.1.66			Solutions shall provide digital rights management capabilities			
SLN9	1	67	SLN9.1.67			Solutions shall provide content publication capabilities including: • Support in-context (what you see is what you get [WYSIWYG]) editing and the ability to preview rendered content in a			
SLN9	1	68	SLN9.1.68			Solutions shall provide check in/check out functionality for electronic documents			
SLN9	1	69	SLN9.1.69			Solutions shall provide notification features for files that are checked out (over due, availability, etc.)			
SLN9	1	70	SLN9.1.70			For document management functions, solutions shall utilize a centralized, shared document management/content management solution.			
SLN9	1	71	SLN9.1.71			Solutions will ensure secure access to electronic records			
SLN9	1	72	SLN9.1.72			Solutions will retain archived records according to state and federal retention guidelines			
SLN9	1	73	SLN9.1.73			Solutions will develop a classification scheme to label records, including electronic record			
SLN9	1	74	SLN9.1.74			Solutions will label records, including electronic records, according to classification scheme			
SLN9	1	75	SLN9.1.75			Solutions will be able to view the latest version or all versions of a document			

SLN9	1	76	SLN9.1.76			Solutions will provide a mechanism to accept and link to documents received in a centralized document management system			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
DBMS

Base	Level	Sub	ReqID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN10	1	1	SLN10.1.1	DBMS		The System shall lock database records based on various parameters (e.g., at row level, field level, or at the application level).			
SLN10	1	2	SLN10.1.2	DBMS		The System shall have the ability to optimize performance in transaction processing versus report processing			
SLN10	1	3	SLN10.1.3	DBMS		The System shall use history tracking within the database and logging options (e.g., transaction auditing)			
SLN10	1	4	SLN10.1.4	DBMS		The System shall assure transaction integrity (e.g., rollback, validity checking, referential integrity, other).			
SLN10	1	5	SLN10.1.5	DBMS		The System shall handle record locking (e.g., row, field, other) and record updating/committing.			
SLN10	1	6	SLN10.1.6	DBMS		Solutions shall support indexing technology (multiple types of Indexing shall be available to tune performance of SQL statement).			
SLN10	1	7	SLN10.1.7	DBMS		Solutions shall provide the ability to optimize individual queries and support parallelizing a query to run on multiple CPUs at the same time to increase performance.			
SLN10	1	8	SLN10.1.8	DBMS		Solutions shall manage multiple query queue entries in parallel.			
SLN10	1	9	SLN10.1.9	DBMS		Solutions shall offer tools to manage and control disparate mixed workloads in a Database Management Solution (DBMS) environment.			
SLN10	1	10	SLN10.1.10	DBMS		The RDBMS must have the ability to maintain security based upon appropriate roles			
SLN10	1	11	SLN10.1.11	DBMS		The RDBMS must have data replication capabilities to external file formats or other RDBM Systems.			
SLN10	1	12	SLN10.1.12	DBMS		The System shall accommodate separate instances of databases.			
SLN10	1	13	SLN10.1.13	DBMS		Solutions shall have full and incremental backup and recovery capabilities on both a regular schedule and an ad hoc basis, including redundant offsite back-ups.			
SLN10	1	14	SLN10.1.14	DBMS		Provide the capability to allow for the continued use of the system during back-ups.			
SLN10	1	15	SLN10.1.15	DBMS		The RDBMS must support geo-encode address data and store geo-data coordinates (longitude and latitude).			
SLN10	1	16	SLN10.1.16	DBMS		Solutions shall assist the State in developing procedures to ensure that specified data is archived and protected from loss, unauthorized access, or destruction.			
SLN10	1	17	SLN10.1.17	DBMS		Solutions shall maintain all data according to state defined records retention guidelines.			
SLN10	1	18	SLN10.1.18	DBMS		Solutions shall maintain all images and electronic documents according to state defined document retention guidelines.			
SLN10	1	19	SLN10.1.19	DBMS		Solutions shall provide on-line access of up to 60 months of data to be used for processing eligibility. Note: Vermont needs to validate # of months			
SLN10	1	20	SLN10.1.20	DBMS		The System shall support online modifications to database structures with minimal user downtime.			
SLN10	1	21	SLN10.1.21	DBMS		The System shall allow for data and transaction replication including, but not limited to, copying an instance of any database to specified locations (e.g. SAN, Multi-site implementations)			
SLN10	1	22	SLN10.1.22	DBMS		The System shall provide standard data extraction API to allow import and export of data.			
SLN10	1	23	SLN10.1.23	DBMS		The System shall provide documented best practices including but not limited to optimum database configuration, client maintenance and change control.			
SLN10	1	24	SLN10.1.24	DBMS		The System shall handle load balancing and/or clustering ability for extended scalability and performance			
SLN10	1	25	SLN10.1.25	DBMS		The System shall avail the capacity planning model for database configuration.			
SLN10	1	26	SLN10.1.26	DBMS		The System supports advanced configurations for data caching (e.g., support of client/application caching, support of server caching etc)			
SLN10	1	27	SLN10.1.27	DBMS		The business analytics solution shall not impact transactional database performance.			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
Technical Architecture

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Req Notes	Requirement Fulfilled?	Requirement Fulfillment Evidence
SLN11	1	1	SLN11 1.1	Business Intelligence		The standard business intelligence tool shall be Oracle Business Intelligence EE with the BI Management Pack, Contact Center Telephony Analytics, Service Analytics, Partner Analytics, and Case Management Analytics compatible with the standard database.			
SLN11	1	2	SLN11 1.2	BPM Suite		The standard BPM suite shall be Oracle Unified Business Process Management Suite			
SLN11	1	3	SLN11 1.3	Content management		The standard Content Management tool shall be Oracle WebCenter Suite Plus which adds the following components: Document Management, Web Content Management (WCM), Digital Asset Management (DAM), Records Management, WebCenter Content Conversion, Java SE, and WebCenter Imaging			
SLN11	1	4	SLN11 1.4	Database		The standard database management system (DBMS) shall be Oracle Database EE with the following add-ons: Real Application Clusters, Advanced Security, Active Data Guard, Diagnostics Pack, Tuning Pack, Change Management pack, Provisioning and Patch Automation Pack, Configuraiton Management Pack for Oracle database, Data Masking Pack, Database Vault, Security Enterprise Search, and Secure Enterprise Search Connector for Siebel			
SLN11	1	5	SLN11 1.5	Data Integration Tools / ETL		The standard ETL and data warehousing tools shall be Oracle Data Integrator/Infromatica Power Center and Oracle Warehouse Builder			
SLN11	1	6	SLN11 1.6	Identity Management		The standard Identity Management platform shall be Oracle Identity and Access Management Suite Plus			
SLN11	1	7	SLN11 1.7	Master Data Management Tool		The standard MDM technology components shall be Oracle Customer Hub Data Steward + B2B + B2C, Oracle Activity Hub B2B + B2C			
SLN11	1	8	SLN11 1.8	Portal		The standard tool for developing portal solutions shall be Oracle WebCenter Suite. The LifeRay portal may be used to support HBE and IE-specific functionality			
SLN11	1	9	SLN11 1.9	Rules Management		The standard rules management platform shall be Oracle Policy Automation, Oracle Policy Automation, and Oracle Policy Automation Connector for Siebel			
SLN11	1	10	SLN11 1.10	SOA Solution		The standard SOA technology components shall be Oracle SOA Suite and related Fusion Middleware (FMW)			
SLN11	1	11	SLN11 1.11	SOA Governance		The standard repository and service registry tools shall be Oracle's Enterprise Repository and Service Registry			
SLN11	1	12	SLN11 1.12	CRM		The standard solution for CRM/Case Management/Call Center shall be the following Siebel components: CRM Base, Public Sector CRM Base, Siebel Tools, Public Sector Partner Portal, Partner Portal, Financial Services CRM Base Option, and Public Sector eService			
SLN11	1	13	SLN11 1.13	Application Server		The standard JEE application server shall be Oracle WebLogic Server (OWLS)			
SLN11	1	14	SLN11 1.14	CTI Component		The standard CTI component shall beSiebel CTI			
SLN11	1	15	SLN11 1.15	CRM Data Quality		The standard data quality component for Siebel shall beSiebel Data Quality			
SLN11	1	16	SLN11 1.16	CRM Call Answering and Service		The standard CRM call answering service shall be Siebel Smart Answer Connector & Service			
SLN11	1	17	SLN11 1.17						
SLN11	1	18	SLN11 1.18	CRM Email Response		The standard email response component for CRM shall be Siebel Email Response			
SLN11	1	19	SLN11 1.19	CRM HelpDesk		The standard help desk component for Siebel shall beSiebel HelpDesk Option			
SLN11	1	20	SLN11 1.20	CRM Group Policy		The standard group policy component shall be CRM Group Policies			
SLN11	1	21	SLN11 1.21	Siebel Individual Coverage		The standard componet for tracking individual coverage shall be Siebel Individual Coverage			

SLN11	1	22	SLN11 1.22	CRM Web Channel for Customers		The standard web channel for CRM shall be Siebel CRM Web Channel for Customers			
SLN11	1	23	SLN11 1.23	CRM Test Automation		The standard Siebel test automation component shall be CRM Test Automation Interfaces			
SLN11	1	24	SLN11 1.24	CRM Remote Client		The standard remote client for CRM shall be Siebel Remote Client			
SLN11	1	25	SLN11 1.25	CRM Field Service		The standard field service component shall be CRM Field Service			
SLN11	1	26	SLN11 1.26	CRM Scheduler		The standard CRM scheduling component shall be Oracle Real-time Scheduler			
SLN11	1	27	SLN11 1.27	Data Quality		The standard data quality modules shall be Oracle Enterprise Data Quality Match & Merge, Parsing & Standardization, Profile & Audit, and Address Validation Server			
SLN11	1	28	SLN11 1.28	User Training Playback		The standard user training playback tool shall be Oracle User Productivity Kit (UPK) Enterprise User and Developer			
SLN11	1	29	SLN11 1.29	Application Integration		The standard application integration toolkit shall be Oracle Oracle Customer Master Data Management Integration Base Pack, Oracle AIA Foundation Pack, Oracle Customer Master Data Management Integration Option for Siebel CRM, and Siebel Field Service Integration to Oracle Real-time Scheduler			
SLN11	1	30	SLN11 1.31	Application Managmement		The standard application management pack for CRM shall be Oracle Application Management Suite for Siebel			
SLN11	1	31	SLN11 1.32	Application Server		The standard application server shall be Oracle WebLogic Suite			
SLN11	1	32	SLN11 1.33	SOA Management		The standard soa management pack shall be Oracle SOA Management Pack EE			
SLN11	1	33	SLN11 1.34	Application Server management		The standard application server management component shall be Oracle Weblogic Server Management pack EE			
SLN11	1	34	SLN11 1.35	Audit Components		The standard database audit tools shall be Oracle Audit Vault Server and Collection Agent			
SLN11	1	35	SLN11 1.36	Portal Management		The standard portal management component shall be Oracle Management Pack for WebCenter Suite			
SLN11	1	36	SLN11 1.37	SOA Healthcare Adapter		The standard healthcare integration components for SOA shall be Oracle Healthcare Adapter			
SLN11	1	37	SLN11 1.38	Content Management Integration		The standard content management adapters shall be Oracle WebCenter Applications Adapter for Siebel and WebCenter Adapter for Microsoft			
SLN11	1	38	SLN11 1.39	Identity Analytics		The standard IdM analytics component shall be Oracle Identity Analytics			
SLN11	1	39	SLN11 1.40	IdM Connectors		The standard IdM Connectors shall be Oracle's connectors for Oracle DBMS Tables, Oracle DBMS, MSFT AD, MSFT Exchange, PSFT Enterprise Applications, MSFT Windows, Unix, RSA Authentication Manager, Siebel Enterprise Applications, and IBM RACF			
SLN11	1	40	SLN11 1.41	IdM Management		The standard IdM management component shall be Oracle Management Pack Plus for Identity Management			
SLN11	1	41	SLN11 1.42	OneGate		The standard external facing portal for Exchange and Integration Eligibility capabilities shall be Exeter OneGate suite. this solution supports the Citizen view, Small Business view, Broker view, Navigator view, and Customer Service view (or exchange data/content) and contains adapters/connectors to Sieble and LifeRay web portal.			
SLN11	1	42	SLN11 1.42	Thunderhead		The standard correnspondence management tool shall be Thurderhead suite that enables the generation and management of official letters/correspondece to potential enrollees, enrollees, navigators, employers, brokers, and state administrators.			
SLN11	1	43	SLN11 1.42	RightFax		The standard fax tool for inbound faxes shall be RightFax from individuals (enrollees, potential enrollees, navigators, employers, and brokers) providing appropriate documentation supporting their health insurance needs, this tool will collect the inbound faxes, integrate with the Enterprise Content Mangaement tool (via SOA adapter) for document storage, and fax processing workflow.			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Useability

Base	Level	Sub	Req ID New	Focus	Specific	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN12	1	1	SLN12.1.1			Solutions will adhere to the accessibility standard as outlined in the web guidelines and based on the W3C level 2 accessibility guidelines: (http://www.w3.org/TR/WCAG10/full-checklist.html).			
SLN12	1	2	SLN12.1.2			Solutions shall allow the users to easily navigate to a variety of functions available to them without having to move sequentially through excessive menus and screens.			
SLN12	1	3	SLN12.1.3			Solutions shall support undo and redo.			
SLN12	1	4	SLN12.1.4			Solutions shall provide users with a clearly marked emergency exit for the instances when a user mistakenly chooses a function and such emergency exit must be simple with minimal dialogue.			
SLN12	1	5	SLN12.1.5			Solutions shall follow standardized conventions and limit the use of words, situations, or actions that have multiple meanings.			
SLN12	1	6	SLN12.1.6			Solutions shall eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.			
SLN12	1	7	SLN12.1.7			Solutions shall minimize the user's memory load by making objects, actions, and options visible.			
SLN12	1	8	SLN12.1.8			Solutions shall provide the option to have rollover / tooltip help or context messages and provide the option to turn off this option in the user preferences profile.			
SLN12	1	9	SLN12.1.9			Solutions shall provide all Solution instructions in a visible or easily retrievable location, when appropriate.			
SLN12	1	10	SLN12.1.10			Solutions shall cater to both inexperienced and experienced users and shall provide accelerators to speed up the interaction for the expert user.			
SLN12	1	11	SLN12.1.11			Solutions will allow users to create shortcuts for frequent actions.			
SLN12	1	12	SLN12.1.12			Solutions shall adhere to all Federal and Vermont accessibility requirements, or their successors: (section 508 of the Rehabilitation Act and detailed in section 1194.22 of the Code of Federal Regulations, Web-based intranet and internet information and applications.			
SLN12	1	13	SLN12.1.13			Solutions's error messages shall be expressed in plain language, precisely indicate the problem, and constructively suggest a solution.			
SLN12	1	14	SLN12.1.14			Solutions shall use colors to enhance user experience and Solution usability while complying with all disability requirements notated elsewhere in these requirements.			
SLN12	1	15	SLN12.1.15			Solutions shall allow the user to navigate to any functional component from a client landing page.			
SLN12	1	16	SLN12.1.16			Solutions shall alert the user with information relevant to required next steps.			
SLN12	1	17	SLN12.1.17			Solutions shall provide drop down and list boxes for all key entry, and text entry will display existing values for selection (auto fill).			
SLN12	1	18	SLN12.1.18			Solutions shall accommodate point and click selection and check box entry for all relevant data entries.			
SLN12	1	19	SLN12.1.19			Solutions shall facilitate data entry and shall contain pop-up list boxes for all code fields in all processing windows and allow selection of the entry with use of hot keys.			
SLN12	1	20	SLN12.1.20			Solutions shall provide field level on-screen edits with limited user override capabilities.			
SLN12	1	21	SLN12.1.21			Solutions shall provide the ability to make fields visible/invisible depending on parameters.			
SLN12	1	22	SLN12.1.22			Solutions shall not show fields not accessible to a given user based on access rights, nor shall Solutions show fields not in use.			
SLN12	1	23	SLN12.1.23			Solutions shall permit all users (dependent on role-based security and access rights) to have current and up to date information regarding Client's information when connected to solutions given the operational and technical constraints of the data source(s). The data displayed must be time stamped to reflect the currency of the data.			
SLN12	1	24	SLN12.1.24			Solutions cursor shall automatically advance to the next logical input field when the maximum allowed numbers of characters have been entered for the keyed field.			
SLN12	1	25	SLN12.1.25			Solutions shall provide the option of having a selection from the drop down boxes automatically take the user to the next field.			
SLN12	1	26	SLN12.1.26			Solutions shall provide validation checks by methods described within policy, functional, and detailed requirements.			
SLN12	1	27	SLN12.1.27			Solutions shall identify invalid entries to the user as immediately as possible.			
SLN12	1	28	SLN12.1.28			Solutions shall provide the ability to suggest or automatically change entries that do not conform to data entry standards.			
SLN12	1	29	SLN12.1.29			Solutions shall be designed to include only the necessary information and functionality on screens and shall be based on the user's access level and the user's configuration.			
SLN12	1	30	SLN12.1.30			Solutions shall be designed to include logical transitions between screens and level of detail during navigation.			
SLN12	1	31	SLN12.1.31			Solutions shall provide templates for data entry with identified mandatory and optional data fields.			
SLN12	1	32	SLN12.1.32			Solutions shall allow incomplete data sets to be saved for completion of the workflow at a later time.			
SLN12	1	33	SLN12.1.33			Solutions shall highlight and flag required and incomplete data fields.			
SLN12	1	34	SLN12.1.34			Solutions shall provide a user interface that shall be simple and consistent throughout all areas and functions of Solutions.			
SLN12	1	35	SLN12.1.35			Solutions shall include a graduated Solution of alert levels to allow users to determine urgency and relevancy.			
SLN12	1	36	SLN12.1.36			Solutions shall allow configuration of alerts by a user, for a user by a supervisor, and for a user by a Solution administrator			

SLN12	1	37	SLN12.1.37			Solutions shall allow for the request of or entry of data from external devices (e.g. tablets, kiosks, barcode scanner, RFID scanner, speech).			
SLN12	1	38	SLN12.1.38			Solutions shall notify the user when a source Solution is unavailable / inoperable and notify user that any available information about the subject being viewed is as of certain time and date.			
SLN12	1	39	SLN12.1.39			Solutions's web interface shall be Web 2.0 compliant			
SLN12	1	40	SLN12.1.40			Solutions shall not require users to reenter data due to validation errors			
SLN12	1	41	SLN12.1.41			Solutions shall enable central workflow alerts and transactional status. Solutions shall centralize pending work items for the user as in a work queue			
SLN12	1	42	SLN12.1.42			Solutions shall support multi-language ***Open action item to identify which languages and whether right to left functionality is required to be supported			
SLN12	1	43	SLN12.1.43			Solutions shall have the capability to push messages to the intended workers without requiring them to specifically inquire for the data.			
SLN12	1	44	SLN12.1.44			Solutions shall provide a hover option over state defined fields to generate a description of the data element.			
SLN12	1	45	SLN12.1.45			Solutions shall minimize the number of mouse clicks / user interaction to complete any action.			
SLN12	1	46	SLN12.1.46			Solutions shall provide auto completion functionality for user defined fields.			
SLN12	1	47	SLN12.1.47			Solutions shall provide linked access to help functions which contain the appropriate information and search of all help information from every window, based on user profiles.			
SLN12	1	48	SLN12.1.48			Solutions shall use a Graphical User Interface (GUI) to help the user navigate to the next logical step in the workflow, or freely navigate to other parts of Solutions's functionality, and then allow the user to return to complete the in-process task.			
SLN12	1	49	SLN12.1.49			Solutions shall preserve context by limiting abrupt transitions and redisplays in order to maximize and enhance the user experience and solution usability.			
SLN12	1	50	SLN12.1.50			Solutions shall speak the users' language, with words, phrases and concepts familiar to the user, rather than solution-oriented terms.			
SLN12	1	51	SLN12.1.51			Solutions shall follow real-world Vermont conventions, making information appear in a natural and logical order.			
SLN12	1	52	SLN12.1.52	Customer Service		Creating and maintaining consumer assistance tools, including a website through which enrollees and prospective enrollees of qualified health benefit plans may obtain standardized comparative information on such plans, a toll-free telephone hotline to respond to requests for assistance, and interactive online communication tools, in a manner that complies with the Americans with Disabilities Act.			
SLN12	1	53	SLN12.1.53	Customer Service - Admin Tasks		Solutions shall include graphics capability for notifications			
SLN12	1	54	SLN12.1.54	Customer Service		Information must be provided to applicants and enrollees in plain language and in a manner that is accessible and timely to— (1) Individuals living with disabilities including accessible Web sites and the provision of auxiliary aids and services at no cost to the individual in accordance with the Americans with Disabilities Act and section 504 & 508 of the Rehabilitation Act. (2) Individuals who are limited English proficient through the provision of language services at no cost to the individual, including (i) Oral interpretation; (ii) Written translations; and (iii) Taglines in non-English languages indicating the availability of language services.			
SLN12	1	55	SLN12.1.55	Financial Management		The Financial system shall incorporate features designed to reduce the amount of direct keying required to initiate transaction processing, such as the following: the use of default values, look-up tables, automatic data recall, single-function windows (e.g., one input screen per transaction), the ability to pass common data from screen to screen, highlighting of required fields, auto tabs, the ability to retrieve suspended transactions by user-type, document, account, and transaction entry undo/redo.			
SLN12	1	56	SLN12.1.56	General		The Financial system shall incorporate graphical user interface characteristics, such as the following: mouse-activated icons, buttons, scroll bars, drop-down lists, check boxes, menu bars, text boxes, tool tips, resizable windows, and cut, copy, and paste functions and undo/redo functionality			
SLN12	1	57	SLN12.1.57	General		The Solution shall allow a search based on one single criteria or multiple search criteria			
SLN12	1	58	SLN12.1.58	Customer Service - Call Center		The system shall provide speech and hearing impaired customers with the ability to communicate through a Teletypewriter (TTY) or Telecommunications Display Device (TDD).			

EA Application Architecture

Health Benefits Exchange Software Requirements

Product	Useage	Vermont ULA	CGI Validation
Siebel CRM Base		X	Yes (as defined by Oracle)
Siebel Public Sector CRM Base Option		X	Yes (as defined by Oracle)
Siebel Tools		X	Yes (as defined by Oracle)
Siebel Public Sector Partner Portal		X	Yes (as defined by Oracle)
Siebel Partner Portal		X	Yes (as defined by Oracle)
Siebel Public Sector eService		X	Yes (as defined by Oracle)
Siebel Financial Services CRM Base Option		X	Yes (as defined by Oracle)
Siebel CTI		X	Yes (as defined by Oracle)
Siebel Data Quality		X	Yes (as defined by Oracle)
Siebel Smart Answer Connector		X	Yes (as defined by Oracle)
Siebel Smart Answer for Service		X	Yes (as defined by Oracle)
Siebel Email Response		X	Yes (as defined by Oracle)
Siebel HelpDesk Option		X	Yes (as defined by Oracle)
Siebel Group Policies		X	Yes (as defined by Oracle)
Siebel Individual Coverage		X	Yes (as defined by Oracle)
Siebel CRM Web Channel for Customers - up to 15 Objects		X	Yes (as defined by Oracle)
Siebel Test Automation Interfaces		X	Yes (as defined by Oracle)
Siebel Remote Client		X	Yes (as defined by Oracle)
Siebel Field Service		X	Yes (as defined by Oracle)
Oracle Real-time Scheduler		X	Yes (as defined by Oracle)
Siebel Email/Web Offer Designer		These are the Siebel CRM email and campaign mangement products that could replace Thunderhead. These are for the Health Connect and are the marketing solutions to fully leverage the CRM database for client correspondances and campaign management to help target Health Connect clients and drive enrollment.	Maybe, required for other internal functions?
Siebel Email Marketing Server			requirements
Siebel Campaign Management			Not required based on current requirements
Siebel Web Marketing			Not required based on current requirements
Siebel Marketing Server			Not required based on current requirements

Product		Vermont ULA	
MDM and Oracle Enterprise Data Quality (EDQ) - to replace Vermont's current investment in Informatica Data Quality quantity based			
Oracle Customer Hub Data Steward		X	Yes (as defined by Oracle)
Oracle Customer Hub B2B		X	Yes (as defined by Oracle)
Oracle Customer Hub B2C		X	Yes (as defined by Oracle)
Oracle Activity Hub B2B for Oracle Customer Hub B2B		X	Yes (as defined by Oracle)
Oracle Activity Hub B2C for Oracle Customer Hub B2C		X	Yes (as defined by Oracle)
Oracle Enterprise Data Quality Match and Merge		X	Yes (as defined by Oracle)
Oracle Enterprise Data Quality Parsing and Standardization		X	Yes (as defined by Oracle)
Oracle Enterprise Data Quality Profile and Audit		X	Yes (as defined by Oracle)
Oracle Data Quality Address Validation Server		X	Yes (as defined by Oracle)

Product		Vermont ULA	
Oracle Policy Automation			
Oracle Policy Modeling		X	Yes (as defined by Oracle)
Oracle Policy Automation		X	Yes (as defined by Oracle)

Oracle Policy Automation Connector for Siebel		X	Yes (as defined by Oracle)
User Productivity Kit (UPK)		***Vermont ULA***	
UPK Enterprise User		X	Yes (as defined by Oracle)
UPK Developer		X	Yes (as defined by Oracle)
Product		***Vermont ULA***	
Application Integration Architecture (AIA)			
Oracle Customer Master Data Management Integration Base Pack		X	Yes (as defined by Oracle)
Oracle Application Integration Architecture Foundation Pack		X	Yes (as defined by Oracle)
Oracle Customer Master Data Management Integration Option for Siebel CRM		X	Yes (as defined by Oracle)
Siebel Field Service Integration to Oracle Real-Time Scheduler		X	Yes (as defined by Oracle)
Product		***Vermont ULA***	
Oracle Business Intelligence Enterprise Edition (OBIEE) and Siebel BI Analytics			
Business Intelligence Publisher		X	Yes (as defined by Oracle)
Oracle Business Intelligence Suite Enterprise Edition Plus		X	Yes (as defined by Oracle)
Informatica PowerCenter and Power Connect Adapters		X	Yes (as defined by Oracle)
Business Intelligence Management Pack		X	Yes (as defined by Oracle)
Contact Center Telephony Analytics		X	Yes (as defined by Oracle)
Service Analytics		X	Yes (as defined by Oracle)
Partner Analytics		X	Yes (as defined by Oracle)
Case Management Analytics		X	Yes (as defined by Oracle)
Product		***Vermont ULA***	
Oracle Database			
Oracle Database Enterprise Edition		X	Yes (as defined by Oracle)
Real Application Clusters		X	Yes (as defined by Oracle)
Advanced Security		X	Yes (as defined by Oracle)
Oracle Active Data Guard		X	Yes (as defined by Oracle)
Diagnostics Pack		X	Yes (as defined by Oracle)
Tuning Pack		X	Yes (as defined by Oracle)
Change Management Pack· (now called database lifecycle management pack(		X	Yes (as defined by Oracle)
Provisioning and Patch Automation Pack for Database		X	Yes (as defined by Oracle)
Configuration Management Pack for Oracle Database		X	Yes (as defined by Oracle)
Oracle Data Masking Pack		X	Yes (as defined by Oracle)
Database Vault		X	Yes (as defined by Oracle)
Secure Enterprise Search		X	Yes (as defined by Oracle)
Secure Enterprise Search Connector - Siebel		X	Yes (as defined by Oracle)
Product		***Vermont ULA***	
Oracle Fusion Middleware/SOA			
Oracle Application Management Suite for Siebel		X	Yes (as defined by Oracle)
WebLogic Suite		X	Yes (as defined by Oracle)
SOA Management Pack Enterprise Edition		X	Yes (as defined by Oracle)
WebLogic Server Management Pack Enterprise Edition		X	Yes (as defined by Oracle)
SOA Suite for Oracle Middleware		X	Yes (as defined by Oracle)
Unified Business Process Management Suite		X	Yes (as defined by Oracle)
Audit Vault Server		X	Yes (as defined by Oracle)
Audit Vault Collection Agent		X	Yes (as defined by Oracle)

Management Pack for WebCenter Suite		X	Yes (as defined by Oracle)
WebCenter Suite		X	Yes (as defined by Oracle)
Enterprise Repository		X	Yes (as defined by Oracle)
Service Registry		X	Yes (as defined by Oracle)
Healthcare Adapter		X	Yes (as defined by Oracle)
Oracle WebCenter Suite Plus – this is an "upgrade" to the State's current investment of WebCenter. Suite Plus includes Document Management, Web Content Management (WCM), Digital Asset Management (DAM), Records Management, WebCenter Content Conversion, Java SE, and WebCenter Imaging. *(NOTE: CGI bid the component functionality for document/content management including: WebCenter Imaging, WebCenter Content, and WebCenter Adapter for Siebel)*		X	Yes (as defined by Oracle)
WebCenter Applications Adapter for Siebel		X	Yes (as defined by Oracle)
WebCenter Adapter for Micrcosoft		X	Yes (as defined by Oracle)
Oracle Data Integrator Enterprise Edition		???	Yes (as defined by Oracle)
Informatica Power Center (ETL Engine)		X	Yes (as defined by Oracle)
Product		***Vermont ULA***	
Oracle Identity and Access Management			
Identity Analytics		X	Yes (as defined by Oracle)
Identity and Access Management Suite Plus		X	Yes (as defined by Oracle)
Identity Manager Connector - Database Applications Table		X	Yes (as defined by Oracle)
Identity Manager Connector - Database User Management		X	Yes (as defined by Oracle)
Identity Manager Connector - Microsoft Active Directory		X	Yes (as defined by Oracle)
Identity Manager Connector - Microsoft Exchange		X	Yes (as defined by Oracle)
Identity Manager Connector - PeopleSoft Enterprise Applications		X	Yes (as defined by Oracle)
Identity Manager Connector - Microsoft Windows		X	Yes (as defined by Oracle)
Identity Manager Connector - UNIX		X	Yes (as defined by Oracle)
Identity Manager Connector - RSA Authentication Manager		X	Yes (as defined by Oracle)
Identity Manager Connector - Siebel Enterprise Applications		X	Yes (as defined by Oracle)
Identity Manager Connector - IBM RACF		X	Yes (as defined by Oracle)
Management Pack Plus for Identity Management		X	Yes (as defined by Oracle)
Product		***CGI Purchases on behalf of Vermont***	
CGI Purchased on behalf of State of Vermont			
OneGate		X	Yes
LifeRay		X	Yes
Thunderhead		X	Yes
RightFax		X	Yes

Production Access View

SOV HBE Roles		Public				State Private Network																																			
		Public Web DMZ				Private Web WAN					Private Web WAN Mgmt			Siebel Product Suite			GateWay		ECM			OPA		IdM			Business Intelligence				ESB	Admin			Database		
No.	Role	Liferay	OIM	ESB	FTP	Siebel	BI	IdM	ECM	Liferay Portal	MDM	ESB WAN	ESB VAN	AOM	GateWay etc.	Report	QNXT/GS	WCC	Thunderhead	MDM	App	OPM	OIM/AM	OAM/AM	OID/AD	OBI Pres	Server/Scheduler	ETL	FTP	ESB/OSB/OBR	Siebel App Mgmt	Siebel Admin Console	DAC Client	QNTP	OLAP	IGM
1	Individual	x	x																																						
2	Employee	x	x																																						
3	Employer	x	x		x																																				
4	Navigator	x	x																																						
5	Assisters (in person and remote)	x	x																																						
6	Broker	x	x		x																																				
7	Issuers	x	x	x	x																																				
8	Premium Processor			x	x																																				
9	Health Connectors	x	x																																						
10	Health Guides	x	x																																						
11	Other (VHC Peers, VHC Whisperers)	x	x																																						
12	SOV HBE Staff					x	x	x	x	x								x				x				x															
13	Maximus (outsourced Call Center CSR agents)	x	x			x	x		x																																
14	Plan Administrator					x	x	x	x									x				x				x															
15	Enrollment Administrator					x	x	x	x	x								x				x				x															
16	Overall Website Administrator	x	x			x	x	x	x	x								x				x				x															
17	ESD (Economic Service District Office) Non Healthcare Question Staff Worker					x	x	x	x									x				x				x															
18	DVHA L2 Resolver					x	x	x	x									x				x				x															
19	HAEU (Health Access Eligibility Unit) Staff Worker					x	x	x	x									x				x				x															
20	State Health Care BPS (Benefits Program Specialist)					x	x	x	x									x				x				x															
21	Eligibility Workers in the 12 ESD District Offices					x	x	x	x									x				x				x															
22	DCF (Department of Children and Families) Staff Worker					x	x	x	x									x				x				x															
23	Legal Aid Worker					x	x	x	x									x				x				x															
24	211 Worker					x	x	x	x									x				x				x															
25	DFR (Department of Financial Regulations) Staff Worker					x	x	x	x									x				x				x															
26	Ombudsman	x	x															x				x				x															
27	Anonymous	x	x																																						
28	Project / Developer Team																																								
29	IT Operational Support (CGI & State)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x