AMENDMENT NO. 2

TO

MASTER SERVICES AGREEMENT

This Amendment No. 2 ("Amendment No. 2"), effective as of August 12, 2013 (the "Amendment No. 2 Effective Date"), is made to that certain Master Services Agreement (the "Agreement") first dated as of December 13, 2012, as amended February 28, 2013, 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 Agreement.

WHEREAS, the Parties have determined that a change of Supplier's scope of work is in their respective interests; and

WHEREAS, the Parties have agreed to remove from Statement of Work No. 1 and define the scope of the hosting services in a new Statement of Work No. 4;

WHEREAS, the Parties wish to amend the Agreement to reflect amendments resulting from the expansion of Supplier's scope of work;

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

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

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

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

5. The following assumption is hereby deleted from Exhibit E, and is added to a new section 1.1.7 in Exhibit I – Hosting Services:

   1.1.7 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.

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

Except as modified by this Amendment No. 2, all provisions of the Agreement remain in full force and effect. This Amendment No. 2 is integrated into and forms part of the Agreement as of the Amendment No. 2 Effective Date.

IN WITNESS WHEREOF the parties have executed this Amendment No. 2 as of the Amendment No. 2 Effective Date.

STATE OF VERMONT

By: E-SIGNED by Mark Larson on 2013-08-13 21:18:15 GMT

Name: _____

Type or Print

Title: _____

CGI TECHNOLOGIES AND SOLUTIONS INC.

By: E-SIGNED by Gregg Mossburg on 2013-08-13 20:15:05 GMT

Name: _____

Type or Print

Title: _____

ATTACHMENT 1
Exhibit C

[see attached]

ATTACHMENT 2
Exhibit D

[see attached]

ATTACHMENT 3
Exhibit E

[see attached]

ATTACHMENT 4
Exhibit F

[see attached]

ATTACHMENT 4
Exhibit L

[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's 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 Base Years Grand Total (as defined in Exhibit L (Pricing) in the Table entitled "Summary Cost SOW#1 and SOW#4") (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 Base Years Grand Total.

5. **Final Critical Milestones.** The date by which each Critical Milestone must be met is detailed in the chart below. Determination of whether a Critical Milestone has been met will be made at the SOV's discretion.

	Critical Milestone	HBE Project Date	Proposed Measures (if any)	Liquidated Damages
1	Functionality demonstrated for PM Exchange Components (e.g. QHP Evaluation and Certification, Issuer Portal)	04/5/2013		Medium
2	Functionality demonstrated for E&E Exchange Components (e.g. enrollment processing, verification interfaces, rate calculator)	04/5/2013		Medium
3	Functionality demonstrated for FM Exchange Components (APTC/CSR data reporting, SHOP and individual premium billing)	04/5/2013		Medium
4	Functionality demonstrated for systems supporting Consumer Assistance functions (e.g. CRM, portal access)	04/5/2013		Medium
5	Development of PM Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013		High
6	Development of FM Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013		High

	Critical Milestone	HBE Project Date	Proposed Measures (if any)	Liquidated Damages
7	Development of E&E Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013		High
8	Development of CA Exchange components completed based on completion of Unit Test and migration to Integration instance.	06/3/2013		High
9	Connectivity established for all required Data Services Hub services	06/3/2013		High
10	Hub and partner testing on all Data Services Hub services completed	06/3/2013		Low
11	Iteration 1 VHC Code Drop/Demo and UAT Start	July 29, 2013	20% of October 1 requirements met in code promoted to Staging, SOV Testers have access to UAT	Low
12	Iteration 2 VHC Code Drop/Demo and UAT Start	August 19, 2013	60% of October 1 requirements met in code promoted to Staging, SOV Testers have access to UAT	Medium
13	Iteration 3 VHC Code Drop/Demo and UAT Start	September 9, 2013	90% of October 1 requirements met in code promoted to Staging, SOV Testers have access to UAT	High
14	SIT 1 Complete	August 15, 2013	12% of October 1 scripts pass; IV&V assessment as to whether the test cycle complied with the test plan, the appropriate activities took place and testing was performed in the TEST environment; should material deficiencies be identified in assessment, CGI will correct and resubmit.	Low

	Critical Milestone	HBE Project Date	Proposed Measures (if any)	Liquidated Damages
15	SIT 2 Complete	September 5, 2013	45% of October 1 scripts pass with fewer than 20 Severity 1 defects; IV&V assessment as to whether the test cycle complied with the test plan, the appropriate activities took place and testing was performed in the TEST environment should material deficiencies be identified in assessment, CGI will correct and resubmit.	Medium
16	SIT 3 Complete	September 20 2013	85% of October 1 scripts pass with no Severity 1 defects; IV&V assessment as to whether the test cycle complied with the test plan, the appropriate activities took place and testing was performed in the TEST environment should material deficiencies be identified in assessment, CGI will correct and resubmit.	High
17	Blueprint Testing	September 6 2013	IV&V sign-off on results	High
18	IRS Safeguards compliance (ACA/IRS 1075)	September 15, 2013 (or soonest IRS can audit)	Audit compliance results with no material unresolvable findings or weaknesses	High
19	PCI DSS compliance	September 18, 2013	Audit compliance as indicated by a PCI DSS Attestation of Compliance for Onsite Assessments — Merchants, Version 2.0 form signed by a CGI officer	High
20	Referentia Test Complete and Accepted by 3rd Party	September 18, 2013	3rd party acceptance	Medium
21	Web Site and Call Center Launch	October 1, 2013	100% of requirements as defined in the RTM (D-14) in production, inclusive of any changes in scope mutually reviewed and accepted by both SOV and CGI via the Change Control Board (CCB) process or through mutually agreed upon contingency plans.	High

CGI and SOV agree to negotiate in good faith additional milestones for delivery after October 1, 2013.

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 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.** Supplier and SOV will mutually agree upon the framework and measures that will be established in the Go-Live deliverable (D-30 (or32)) by August 23, 2013.

Exhibit D

Service Levels

1. Generally. The Exchange and associated Hosting Services (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. For avoidance of doubt, the Supplier commitments in this Exhibit D are in addition to and not in lieu or limitation of any Supplier obligations in the MSA. Capitalized terms not defined in this Exhibit D will have the definitions assigned to them in the MSA. References to "Problem Levels" in the MSA shall be deemed to be references to the "Severity Levels" in this Exhibit D as defined below.

2. Summary Table. The following Service Levels and Service Level Credits apply to the Hosting Services (as defined in Statement of Work No. 4 to the MSA), subject to the provisions set forth herein.

Service Level Agreement (SLA)	**Service Level**	**Service Credit for Failure**
Supplier WAN Network Latency	Service Level: 95% within 100ms Egregious Service Level: 98% within 139ms	For each day: $3500 Egregious: $5,000 (only one credit shall apply)
Availability During All Hours	Production: 99.90% Egregious: 94% Non-Production: 99.5% Non-Production Egregious: 94%	For each hour: $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: Maximum of 1 second average	For each day: $1,000
	Egregious: Maximum of 5 second average in any hour 3 times in any day OR Maximum of 5 second average in any hour 10 times in a week	Egregious: $5,000 each day or week
Response Time for Real Time Transactions	Production: 90% within 5 seconds	For each day: $1,000
	Egregious: 75% within 5 seconds or any greater than 10 seconds	Egregious: For each day: $5,000

Service Level Agreement (SLA)	Service Level	Service Credit for Failure
Help Desk Mean Time to Restore Severity Level 1	4 Hours	$5,000 per day
	Egregious: Any greater than 24 Hours	$500 per hour
Help Desk Mean Time to Restore Severity Level 2	8 Hours	$5,000 per day
	Egregious: Any greater than 5 days	Egregious: $500 per hour
Help Desk Mean Time to Resolve Severity Level 3	24 Business Hours unless waived by SOV according to agreed plan identified and agreed as part of problem restore activities. Daily update on status.	$500 per day after the first 24 Business Hours
Help Desk Mean Time to Resolve Severity Level 4	40 Business Hours unless waived by SOV according to agreed plan identified and agreed as part of problem restore activities. Daily update on status.	$300 per day after the first 24 Business Hours

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

3. Service Level Descriptions.

3.1 Supplier WAN Network Latency

(a) Definitions.

(i) "**Latency**" is defined as the One-way latency from source to destination plus the One-way latency from the destination back to the source.

(ii) "**One-way Latency**" is defined as the time from the source sending a packet to the destination receiving it.

(b) Description of Service Level. This Service Level measures daily average Latency.

(c) Measurement. Each day, through an agreed automated process, Supplier will sample Latency no less frequently than every five (5) minutes and compile daily statistics. The source point and the receiving point used in taking the measurement will be designated by SOV.

(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 multiplied by each day that the average is above the Egregious Service Level.

3.2 Availability During All Hours

(a) Definitions.

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

(ii) "**All Hours**" means: All time 7 x 24 each week.

(iii) **"Business Hour**" means the hours from 9:00 AM to 5:00 PM Eastern Time, Monday through Friday.

(iv) **"Minor Maintenance Window"** means every three weeks from 9pm Saturday to 9am Sunday. System Availability will be unaffected during Minor Maintenance Windows. Supplier shall provide SOV notice at least ten (10) days in advance of any Minor Maintenance Window in which Supplier may perform any System maintenance.

(v) **"Major Maintenance Window"** means every three weeks from 9pm Saturday to 9am Sunday and will be subject to notice requirements for Scheduled Maintenance.

(vi) **"Scheduled Maintenance"** means System maintenance described in written notice from Supplier at least thirty (30) days in advance for a Major Maintenance Window that may require unAvailability that is performed within the Minor or Major Maintenance Windows and in accordance with such notice from Supplier, and for which Supplier timely posts a notice of Scheduled Maintenance on the Exchange website according to agreed procedures agreed in writing by Supplier and SOV.

(vii) **"Scheduled Maintenance Downtime"** means any period of unAvailability for Scheduled Maintenance.

(b) **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 Supplier either through alarms, the knowledge of its personnel or a report by SOV or another user. Supplier 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

(c) **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.

3.3 Content Maintenance

(a) **Definitions.**

(i) **"Content"** means all information and materials to be posted on the Exchange website.

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

(c) **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 Exchange website.

(d) **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.

3.4 Web Page Response Time

(a) **Definitions.**

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

(ii) **Description of Service Level.** This Service Level measures daily average time that the Web Pages comprising the Exchange website take to respond to a request sent by a user through the user's browser.

(iii) **Measurement.** Each day, through an agreed automated process, Supplier 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.

(iv) **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.

3.5 Response Time for Real Time Transactions

(a) **Definitions.**

(i) **"Real Time Transaction"** means a transaction between a user of the Exchange 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.

(b) **Description of Service Level.** This Service Level measures daily average time that the Web Pages comprising the Exchange 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, Supplier 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.

(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 multiplied by each day that the average is above the Egregious Service Level.

3.6 Help Desk Mean Time to Resolve Severity Level 1

(a) **Definitions.**

(i) **"Severity Level 1 Incident"** means an Incident that is characterized by the following attributes: the Incident (a) renders a business critical System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

(ii) **"Incident"** means any malfunction or defect that causes or is likely to cause or result in the System to fail to conform to the Requirements.

(iii) **"Restore"** means that Supplier has done one of the following: (i) Correct the Incident to restore the System to normal functionality in conformity with the Requirements; (ii) Provide a Workaround; or (Iii) Correct a portion of the Incident to reduce the Severity Level.

(iv) "**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).

(b) **Description of Service Level.** This Service Level measures the mean time for Supplier to Restore the System from the time the Severity Level 1 Incident is first reported to or discovered by Supplier.

(c) **Measurement.** Supplier's trouble ticketing system will automatically track the time from initiation of the Incident to closure. The Incident ticket will be initiated immediately upon Supplier becoming aware of the Incident. Supplier will notify SOV of the Incident within fifteen (15) minutes of the Severity Level 1 Incident ticket creation by telephone, email or other confirmed means.

(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 multiplied by each hour that is above the Service Level.

3.7 Help Desk Mean Time to Resolve Severity Level 2

(a) **Definitions.**

(i) **"Severity Level 2 Incident"** means an Incident that is characterized by the following attributes: the Incident (a) does not render a business critical System, Service, Software, Equipment or network component un-Available or substantially un-Available, but a function or functions are not Available, substantially Available or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

(b) **Description of Service Level.** This Service Level measures the mean time for Supplier to Restore the System from the time the Severity Level 2 Incident is first reported to or discovered by Supplier.

(c) **Measurement.** Supplier's trouble ticketing system will automatically track the time from initiation of the Incident to closure. The Incident ticket will be initiated immediately upon Supplier becoming aware of the Incident. Supplier will notify SOV of the Incident within one (1) hour of the Severity Level 2 Incident ticket creation by telephone, email or other confirmed means.

(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 multiplied by each hour that is above the Service Level.

3.8 Help Desk Mean Time to Resolve Severity Level 3

(a) **Definitions.**

(i) **"Severity Level 3 Incident"** means an Incident that is characterized by the following attributes: the Incident causes a group or individual to experience

a Incident with accessing or using a System, Service, Software, Equipment or network component or a key feature thereof and a reasonable workaround is not available, but does not prohibit the execution of productive work.

(ii) **"Resolve"** means that Supplier has fixed the root cause of the Incident and removed any Workaround and that SOV has determined that the state reported in the Incident no longer exists.

(b) **Description of Service Level.** This Service Level measures the mean time for Supplier to Resolve Severity Level 3 Incidents from the time first reported to or discovered by Supplier.

(c) **Measurement.** Supplier's trouble ticketing system will automatically track the time from initiation of the Incident to closure. The Incident ticket will be initiated immediately upon Supplier becoming aware of the Incident. Supplier will notify SOV of the Incident within four (4) hours of the Severity Level 3 Incident ticket creation by telephone, email or other confirmed means.

(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 multiplied by each hour that is above the Service Level.

3.9 Help Desk Mean Time to Resolve Severity Level 4

(a) **Definitions.**

(i) **"Severity Level 4 Incident"** means an Incident that is characterized by the following attributes: the Incident may require an extended resolution time as set forth in the chart above, but does not prohibit the execution of productive work and a reasonable workaround is available.

(b) **Description of Service Level.** This Service Level measures the mean time for Supplier to Resolve Severity Level 4 Incidents from the time first reported to or discovered by Supplier.

(c) **Measurement.** Supplier's trouble ticketing system will automatically track the time from initiation of the Incident to closure. The Incident ticket will be initiated immediately upon Supplier becoming aware of the Incident. Supplier will notify SOV of the Incident within eight (8) hours of the Severity Level 4 Incident ticket creation by telephone, email or other confirmed means.

(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 multiplied by each hour that is above the Service Level.

3.10 Backup and Recovery

(a) **Definitions.**

(i) "Backup" means a copy of the data stored in the System used for Recovery purposes. Daily Backups shall commence after 12:00 AM and shall conclude before 4:00 AM.

(ii) **"Recovery"** means the loading of data from a Backup into the appropriate database of the System.

(b) **Description of Service Level.** This Service Level measures completion of the scheduled Backups and of all necessary Recoveries each month.

(c) **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.

(d) **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.

3.11 Batch Completion

(a) **Definitions.**

(i) **"Batch"** means a scheduled program that runs without user intervention. Supplier will maintain a list of all Batch jobs run by the System.

(b) **Description of Service Level.** This Service Level measures completion of scheduled Batch jobs.

(c) **Measurement.** All Batch jobs will be monitored by the System and completion and failure automatically reported.

(d) **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.

3.12 Disaster Recovery

(a) **Definitions.**

(i) **"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.

(ii) **"RPO"** means the Recovery Point Objective, the maximum period for lost data in the event of a Disaster.

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

(b) Description of Service Level. In the event of a Disaster, Supplier will meet the RPO and RTO to recover the System and restore full Availability.

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

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

4. 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; provided that Service Credits for Disaster Recovery shall not count against the cap set forth herein.

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

6. Exclusions. Supplier'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 Supplier is neither better nor worse off in Service Level calculations because of such failure) to the extent that Supplier's failure is caused by one of the following circumstances, so long as Supplier 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 Supplier with its obligations arising under this MSA in connection with such Force Majeure Event); (iii) any circumstance where Supplier is prohibited by applicable Law from taking actions required to correct such failure so long as Supplier 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 a 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 such 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, Supplier 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).

7. Service Level Credits

7.1 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.

7.2 Earn-Back. If in any month Supplier 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 Supplier does not owe any Service Level Credits, then Supplier 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 Supplier having a balance in Earn Back Credits, such Earn Back Credits will expire and have no force or effect.

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

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

8.1 Compliance. Supplier 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.

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

8.3 Trending. Supplier will provide monthly, quarterly and annual SLA trending reports requested by SOV.

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

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

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

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

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

10.2 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.

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

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

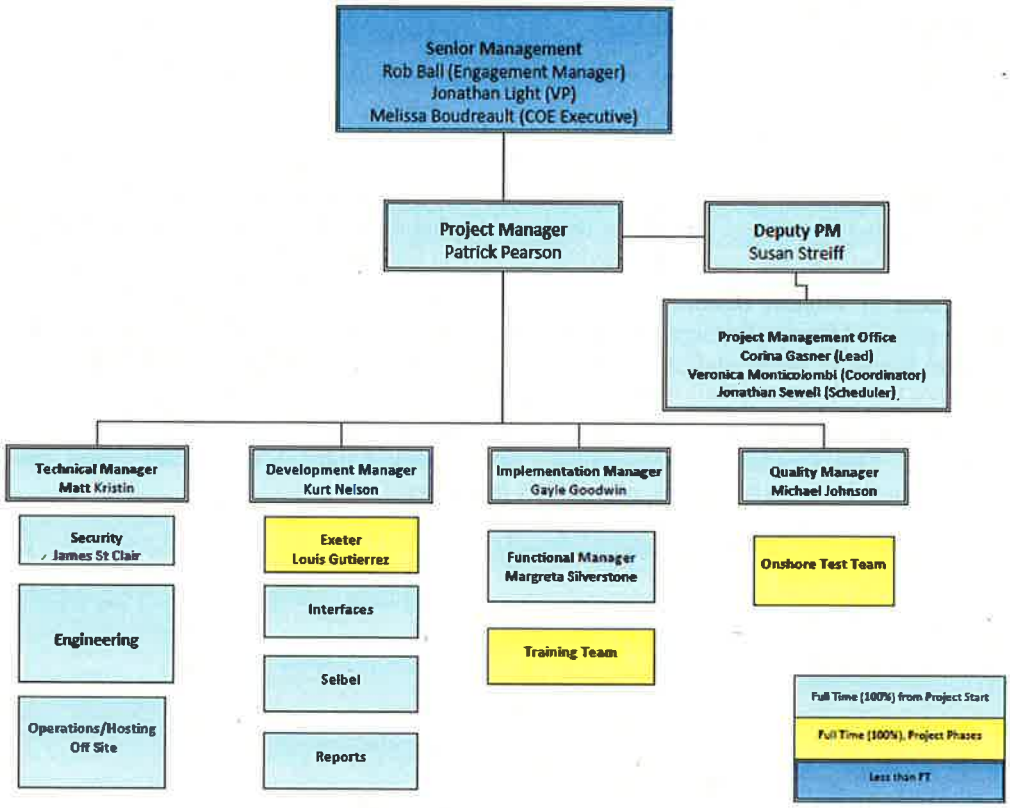
1.1.3. Staffing Assumptions

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 reviewing Project 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

	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.
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 systemtest 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. The Operations & Maintenance Manual details instructions and directions for the Maintenance and Operations (M&O) work that the Supplier's Infrastructure and Application staff need to perform in support of Exchange operations. As guidance the manual must speak to the following areas: • System and Application Accounting (List) • System Backup and Restore Procedures and Schedule • VM to VM cloning Procedures • Patch Procedures and Schedule o Infrastructure o Application • Upgrade Procedures and Schedule o Infrastructure o Application • New Release Procedures and Schedule o Infrastructure o Application • Security o Components o Security Procedures and Audit Schedule o Log File Administration o Breach Incident Reporting • Monitoring and Incident Reporting o Data Storage Growth o Performance

	Description
	• Authentication and Authorization Procedures • Failover and High Availability • Documentation o Systems o Applications o Scheduled Routines and Processes o Procedures Checklists o Topology o Roles • Refresh of the Training Environments • Document Management: o Thunderhead o OPA Rules
(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

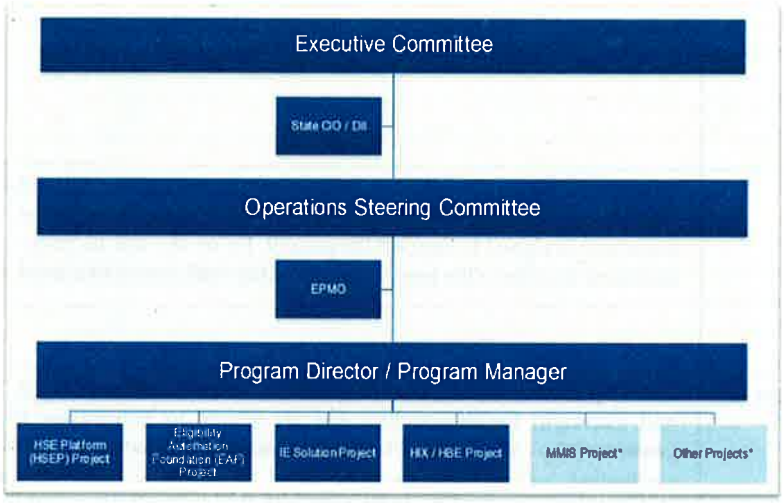
Role	Functions
Project Sponsor	The Project Sponsor assumes project ownership and performs the following functions: Assumes project ownership, and is the highest possible level of project review and provides policy leadership and oversight as needed. Reviews and resolves policy, fiscal, and resource allocation 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

Exhibit F

Security Policies

1. CMS Catalog of Minimum Security Controls for States Supplement, as finalized and amended by CMS from time to time.
2. State of Vermont Security Policies and the Agency of Human Services Security Policies. These policies are available upon request.
3. Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, to the extent not in conflict with 1 and 2 above.
4. IRS Safeguards Program – Publication 1075, FIPS 140-2 and IRS Security Bulletin 1075.
5. HIPAA Security and Privacy Rules as amended by HITECH and as amended from time to time.
6. Any other information technology security policies implemented and/or adopted by SOV, as amended from time to time. These policies are available upon request.
7. Prior to placement of Supplier Personnel on the project, SOV will provide the appropriate level of HIPAA compliance training to Supplier Personnel as deemed necessary by SOV.
8. Security measures requested by DVHA necessary to provide space to the Supplier or access to any SOV Facilities as provided for in Exhibit E or in the MSA.
9. Payment Card Industry – Data Security Standard (PCI-DSS) version 2.0 policies and any subsequent update or amendment thereto.

Pricing Exhibit Table of Contents

Contents of the Pricing Exhibit:

Summary Cost

L-1 Statement of Work 1: Design, Development and Implementation (DDI) of VT HBE

L-1.1 Deliverables and Invoice Amounts
L-1.2 Hourly Rate Table of SOW #1

L-4 Statement of Work 4: Hosting and Maintenance & Operations (M&O)

L-4.1 Monthly DDI Services
L-4.2 License Costs
L-4.3 Annual M&O Services
L-4.4 Hourly Rate Table SOW #4
L-4.5 Environment Cost
L-4.6 Summary Cost of SOW #4

Vermont HBE

Notwithstanding anything herein to the contrary the parties agree that SOV's obligation to make any payment set forth herein, including payment of any monthly fee, license fee, deliverable fee, or milestone-related fee, shall be conditioned upon Supplier's fulfillment of its obligations related to such payment and Supplier's delivery of any deliverable related to such payment, as applicable, in a form and manner satisfactory to SOV.

The table below is a high-level summary of maximum amounts payable in SOW #1 and SOW #4. The figures reflect the sum of the L-1 Tables and L-4 Tables. The Supplier understands that there is no commitment from the SOV to extend the contract term beyond the base years unless it is reduced to writing in an amendment signed by both parties.

Summary Cost SOW#1 and SOW#4

Statement of Work	Total Cost
SOW #1: SI Services	**$ 32,136,258.00**
SOW #4: Hosting	**$ 30,073,712.13**
-Base Years	$ 18,888,671.13
-Optional Years	$ 11,185,041.00
Base Years Grand Total	**$ 51,024,929.13**
Base + Optional Years Grand Total	**$ 62,209,970.13**

The L-1 tabs that follow provide the payment provisions for SOW#1

L-1 PAGE DIVIDER
TABS THAT FOLLOW PROVIDE PAYMENT PROVISIONS FOR SOW #1

Vermont HBE

L-1.1 Deliverables and Invoice Amounts

This table L-1.1 shows the completion dates, expected invoice dates, and invoice amount by deliverable for each Deliverable. The Supplier shall invoice the SOV monthly for the deliverables completed in the previous month. The invoices will be due and payable 30 days following the date on the invoice. All payments are subject to SOV acceptance of completed deliverbales.

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

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

L-1.2 Hourly Rate Table for Change Orders Pertaining to SOW #1

This table L-1.2 includes hourly rates for potential Change Orders.
The Supplier understands that there is no commitment from the SOV to purchase Change Orders.

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

Staff Classifications	Hourly Rate
Technical Lead/DBA	$256.25
Technical Analyst	$218.75
Business/Configuration Analyst	$206.25
Programmer	$193.75
Trainer	$206.25
Technical Writer	$87.50
Tester	$206.25
Security Analyst	$218.75
Senior SME	$281.25
Technical Architect	$331.25
Subject Matter Expert	$243.75

The L-4 tabs that follow provide the payment provisions for SOW#4

Vermont HBE

L-4.1 Monthly Hosting Services During Design, Development and Implementation

This table L-4.1 provides expected monthly amounts for the application support, implmentation of the Hosting Services and the software license maintenance during the DDI period. All payments are subject to SOV acceptance of the Hosting Services.

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

Services	Expected Invoice Date	Invoice Amount	
Usage of the Hosting Services		$ 155,088.00	
Full Implementation of the Dedicated Vblock Hosting Environment		535,732.00	
Software Maintenance		181,653.00	
	3/1/13	**$ 872,473.00**	This payment was based on Amendment 1 costs.
Application Support in Hosting Services		$ 155,088.00	
Full Implementation of Hosting Services		52,854.00	
Software Maintenance		56,910.75	
	4/5/13	**$ 264,852.75**	This payment was adjusted based on overpayment from 3/1/13 and lower costs of Amendment 2
Application Support in Hosting Services		$ 155,088.00	
Full Implementation of Hosting Services		294,293.00	
Software Maintenance		119,281.88	
	5/1/13	**$ 568,662.88**	
Application Support in Hosting Services		$ 155,088.00	
Full Implementation of Hosting Services		294,293.00	
Software Maintenance		119,281.88	
	6/1/13	**$ 568,662.88**	
Application Support in Hosting Services		$ 155,088.00	
Full Implementation of Hosting Services		294,293.00	
Software Maintenance		119,281.88	
	7/1/13	**$ 568,662.88**	
Application Support in Hosting Services		$ 155,088.00	
Full Implementation of Hosting Services		294,293.00	
Software Maintenance		119,281.88	
	8/1/13	**$ 568,662.88**	
Application Support in Hosting Services		$ 155,088.00	
Full Implementation of Hosting Services		294,293.00	
Software Maintenance		119,281.88	
	9/1/13	**$ 568,662.88**	
Application Support in Hosting Services		$ 155,084.00	
Full Implementation of Hosting Services		294,296.00	
Software Maintenance		119,281.88	
	11/7/13	**$ 568,661.88**	
Application Support in Hosting Services		**$ 1,240,700.00**	
Full Implementation of Hosting Services		**$ 2,354,347.00**	
Software Maintenance		**$ 954,255.00**	
Total		**$ 4,549,302.00**	

Vermont HBE
L-4.2 License Costs

This table L-4.2 provides the Liscense costs.

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

Product	Vendor	Description	License Type	License Cost
OneGate	Exeter		Enterprise	$ 5,764,706.00
ALMComplete	SmartBear	- Requirements Management - Defect tracking	38 Concurrent Users	$ 29,348.38
WebLoad	RadView	Load and Performance Testing	1000 Virtual Users	$ 40,000.00
Ensemble	CGI	Internal (CGI) document repository (Issue, Change, Risk, Collaboration, Doc Repository)		$ 19,037.00
ER/Studio	Embarcadero Technologies	Data modeling and metadata management software	3 User License	$ 17,986.00
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	$ 205,275.00
JAWS	Freedom Scientific	- ADA Compliance verification - Usability Testing	1 License	$ 1,264.00
Thunderhead NOW	Thunderhead	Simple Correspondence	300K	$ 222,750.00
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	KeepAutomation		Corporate Developer License Linear 1D + 2D Package	$ 3,694.00
Splunk	splunk.com		500 megabyte-per-	$ 6,928.00
AccVerify	HiSoftware	508 Compliance Check	2 User License for 2 Years	$ 3,169.00
ATSM	CGI	Test Automation and Regression, Case Loading and Support	n/a	$ 36,000.00
Data Masker	Net2000	Test and Development Data creation and manipulation; The one-time license fee for a platform/seat implementation is $4,950 plus first years support of $990 (20% of the license fee) which is mandatory in the first year	1 license	$ 5,940.00
SnagIt	TechSmith	Test Defect Recording and Playback	25 users	$ 779.75
Crossbrowsertesting.com	Crossbrowsertesting.com	Web compatibility	5 Users	$ 500.00
CGI SWAT	CGI	Agile tool, sprint management		$ -
Checkstyle	FOSS/LGGPL	Coding Standards (JAVA)	Open Source	$ -
Cobertura	FOSS/GGPL	Code Coverage (Java)	Open Source	$ -
CSSAnalyzer		Usability Testing Tools	Open Source	$ -
Eclipse	eclipse.org	Java IDE	Open Source	$ -
FindBugs	FOSS/LGGPL	Coding Standards (JAVA)	Open Source	$ -
Google Analytics	Google	Web Analytics	Free	$ -
Javadoc	Oracle	Documentation (Java)	Open Source	$ -
JavaNCSS	FOSS/GGPL	Code Metrics (Java)	Open Source	$ -
Jenkins/Hudson	FOSS/MIT	Continuous Integration Server	Open Source	$ -
Junit	FOSS/CPL	Unit Testing tool	Open Source	$ -
Maven	FOSS/Apache	Build Tool	Open Source	$ -
Quartz	FOSS/Apache		Open Source	$ -
Selenium	FOSS/Apache	Web application record/playback tool used for regression testing of the user interface	Open Source	$ -
SLF4J	FOSS/MIT		Open Source	$ -
SONAR	FOSS/LGGPL	Coding Standards (JAVA) (Code Quality Metrics)	Open Source	$ -
SpringSource	Vmware	Java IDE	Open Source	$ -
Subversion	FOSS/Apache	Version Control	Open Source	$ -
			Subtotal All Items	**$ 6,373,612.13**

Vermont HBE

L-4.3 Annual Maintenance & Operation (M&O) Services

This table L-4.3 provides the fixed Maintenance & Operation (M&O) and Hosting costs for each contract time period. The notes below the table indicate how the monthly amount for each contract period is derived. The Supplier understands that there is no commitment from the SOV to extend the contract term beyond the base years unless it is reduced to writing in an amendment signed by both parties.

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

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 Operations Application Support Services Cost	$	1,994,100.00
	Fixed Operations Hosting Cost	$	2,847,865.00
2	M&O Base Contract Year 2 (10/1/14 - 12/31/14)[2]:		
	Fixed Software Maintenance	$	365,365.00
	Fixed Operations Application Support Services Cost	$	498,520.00
	Fixed Operations Hosting Cost	$	802,625.00
3	M&O Optional Contract Year 1 (1/1/15 - 12/31/15)[1]:		
	Fixed Software Maintenance	$	1,062,537.00
	Fixed Operations Application Support Services Cost	$	1,994,100.00
	Fixed Operations Hosting Cost	$	2,539,448.00
4	M&O Optional Contract Year 2 (1/1/16 - 12/31/16)[1]:		
	Fixed Software Maintenance	$	1,066,873.00
	Fixed Operations Application Support Services Cost	$	1,994,100.00
	Fixed Operations Hosting Cost	$	2,527,983.00
	Total	**$**	**19,150,798.00**

[1] *For Lines 1, 3 and 4 the yearly amount for Fixed Software Maintenance and the Fixed Operations Costs (both Services & Hosting) 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 (both Services & Hosting) will be invoiced monthly in arrears at 1/3 of the amount for the period.*

Table L-4.4 Hourly Rate Table for Change Orders Pertaining to SOW #4

This table L-4.4 includes hourly rates for potential Change Orders.
The Supplier understands that there is no commitment from the SOV to purchase 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 L-4.1 and L-4.2

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

Staff Classifications	Hourly Rate
Technical Lead/DBA	$256.25
Technical Analyst	$218.75
Business/Configuration Analyst	$206.25
Programmer	$193.75
Trainer	$206.25
Technical Writer	$87.50
Tester	$206.25
Security Analyst	$218.75
Senior SME	$281.25
Technical Architect	$331.25
Subject Matter Expert	$243.75

Vermont HBE

L-4.5 Hosting Environment Cost

This table L-4.5 provides the hosting cost by environment, application support cost and software license maintenance costs for each of the delivery time periods.

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

	Environments	VM	App Support	Cloud Infra/Support	Total	
DDI 8mos	Production	50	$ 1,240,700.00	$ 660,966.00	$ 1,901,666.00	
DDI 8mos	Staging	50	$ -	$ 386,871.00	$ 386,871.00	
DDI 8mos	Testing	20	$ -	$ 235,721.00	$ 235,721.00	
DDI 8mos	Training	20	$ -	$ 209,352.00	$ 209,352.00	
DDI 8mos	Development	20	$ -	$ 254,707.00	$ 254,707.00	
DDI 8mos	Disaster Recovery	50	$ -	$ 606,730.00	$ 606,730.00	
		210	$ 1,240,700.00	$ 2,354,347.00	$ 3,595,047.00	total
	Software Maintenance			$ 954,255.00		
	Grand Total			$ 4,549,302.00		
Year 1	Production	50	$ 1,994,100.00	$ 799,518.00	$ 2,793,618.00	
Year 1	Staging	50		$ 467,967.00	$ 467,967.00	
Year 1	Testing	20	$ -	$ 285,132.00	$ 285,132.00	
Year 1	Training	20	$ -	$ 253,237.00	$ 253,237.00	
Year 1	Development	20	$ -	$ 308,099.00	$ 308,099.00	
Year 1	Disaster Recovery	50	$ -	$ 733,912.00	$ 733,912.00	
		210	$ 1,994,100.00	$ 2,847,865.00	$ 4,841,965.00	total
	Software Maintenance			$ 1,457,282.00		
	Grand Total			$ 6,299,247.00		
Yr 2 (3mos)	Production	50	$ 498,520.00	$ 225,331.00	$ 723,851.00	
Yr 2 (3mos)	Staging	50		$ 131,889.00	$ 131,889.00	
Yr 2 (3mos)	Testing	20	$ -	$ 80,360.00	$ 80,360.00	
Yr 2 (3mos)	Training	20	$ -	$ 71,371.00	$ 71,371.00	
Yr 2 (3mos)	Development	20	$ -	$ 86,833.00	$ 86,833.00	
Yr 2 (3mos)	Disaster Recovery	50	$ -	$ 206,841.00	$ 206,841.00	
		210	$ 498,520.00	$ 802,625.00	$ 1,301,145.00	total
	Software Maintenance			$ 365,365.00		
	Grand Total			$ 1,666,510.00		
Year 3	Production	50	$ 1,994,100.00	$ 723,935.00	$ 2,718,035.00	
Year 3	Staging	50		$ 485,701.00	$ 485,701.00	
Year 3	Testing	20	$ -	$ 267,392.00	$ 267,392.00	
Year 3	Training	20	$ -	$ 247,769.00	$ 247,769.00	
Year 3	Development	20	$ -	$ 260,659.00	$ 260,659.00	
Year 3	Disaster Recovery	50	$ -	$ 553,992.00	$ 553,992.00	
		210	$ 1,994,100.00	$ 2,539,448.00	$ 4,533,548.00	total
	Software Maintenance			$ 1,062,537.00		
	Grand Total			$ 5,596,085.00		
Year 4	Production	50	$ 1,994,100.00	$ 717,454.00	$ 2,711,554.00	
Year 4	Staging	50		$ 485,923.00	$ 485,923.00	
Year 4	Testing	20	$ -	$ 250,688.00	$ 250,688.00	
Year 4	Training	20	$ -	$ 245,738.00	$ 245,738.00	
Year 4	Development	20	$ -	$ 258,982.00	$ 258,982.00	
Year 4	Disaster Recovery	50	$ -	$ 569,198.00	$ 569,198.00	
		210	$ 1,994,100.00	$ 2,527,983.00	$ 4,522,083.00	total
	Software Maintenance			$ 1,066,873.00		
	Grand Total			$ 5,588,956.00		

Reconciliation to Exhibit L-2:

Grand Total DDI 8 months (from above)	$ 4,549,302.00
Grand Total Year 1 (from above)	$ 6,299,247.00
Grand Total Year 2 (3 mths) (from above)	$ 1,666,510.00
Grand Total Year 3 (from above)	$ 5,596,085.00
Grand Total Year 4 (from above)	$ 5,588,956.00
Add Software Licenses (presented in L-4 but not above)	$ 6,373,612.13
Total	**$ 30,073,712.13**

Vermont HBE

L-4.6 SOW #4 Summary: Hosting Services

This table L-4.6 summarizes the costs per category in SOW #4. The Supplier understands that there is no commitment from the SOV to extend the contract term beyond the base years unless it is reduced to writing in an amendment signed by both parties.

For avoidance of doubt, as set forth on page 2, all payments are subject to SOV's acceptance for any monthly fee, license fee, deliverable fee, or milestone-related fee.

SOW #4 Summary		
Hosting Services During DDI		
Application Support in Hosting Services	$	1,240,700.00
Full Implementation of Hosting Services	$	2,354,347.00
Software Maintenance	$	954,255.00
License Costs		
Configuration Total	$	6,373,612.13
M&O Hosting Services		
Contract Base Year 1 Total	$	6,299,247.00
Contract Base Year 2 Total	$	1,666,510.00
Optional Contract Year 1	$	5,596,085.00
Optional Contract Year 2	$	5,588,956.00
Grand Total of SOW# 4 Payments (Base Years)	**$**	**18,888,671.13**
Grand Total of SOW# 4 Payments (Base + Option Years)	**$**	**30,073,712.13**

Amended and Restated Statement of Work No. 1

This Amended and Restated Statement of Work Number 1 ("**Statement of Work**" or "**SOW**"), dated as of July __, 2013 (the "**Restatement Date**") and issued pursuant to the Master Services Agreement dated as of December 13, 2012, as amended February 28, 2013, and July __, 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.

0, AMENDMENT AND RESTATEMENT.

SOV and Supplier previously entered into that certain Statement of Work No. 1, dated December 17, 2012 (the "Original SOW#1"). SOV and Supplier desire to amend and restate the Original SOW#1 in its entirety, and, accordingly, this SOW shall supersede and replace the Original SOW#1 as of the Restatement Date.

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 IT Services based on the Functional Requirement Traceability Matrix (the "**Functional RTM**") attached here as Schedule A to this SOW and incorporated herein by reference. Additional specificity regarding the scope of Services is provided for in Exhibit E (Scope Assumptions) to the MSA.

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.

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 executing this SOW, 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 SOW # 4.

4. PROJECT MANAGERS.

See Exhibit E (Scope Assumptions) to the MSA.

5. STAFF.

A. Subcontractors.

Supplier has engaged 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.

Not applicable to this SOW.

7. HARDWARE.

Not applicable to this SOW.

8. THIRD PARTY CONTRACTS.

Not applicable to this SOW.

9. SERVICE LEVELS.

See SOW # 4.

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

As required by 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.

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

14. OPTIONAL SERVICES.

Not applicable to this SOW.

15. OTHER SERVICES.

Not applicable to this SOW

16. CHARGES AND PASS-THROUGH EXPENSES.

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

Agreed to and accepted by:

CGI Technologies and Solutions Inc. (CGI)	State of Vermont
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

SCHEDULE A

Functional RTM

[see attached]

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-001	Plan Management	N/A	OneGate	Provide a business rules engine that can support Exchange, State and federal Plan Management rules	Validated
PM-002	Plan Management	N/A	OneGate	Provide a business rules engine that allows trained authorized business users to configure Exchange rules	Validated
PM-003	Plan Management	N/A	OneGate	Provide the ability define a begin and end date for a plan enrollment period	Validated
PM-004	Plan Management	N/A	OneGate	Allow for multiple enrollment periods during a calendar year.	Validated
PM-005	Plan Management	N/A	OneGate	Provide the ability open a special enrollment period to enable enrolling a plan outside the defined enrollment period.	Validated
PM-006	Plan Management	Initiate QHP Issuer App	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.	Deleted
PM-007	Plan Management	Initiate QHP Issuer App	SERFF	Provide the ability for Issuers to submit an electronic Notification of Issuer's Intent to Apply, including all mandatory information	Deleted
PM-008	Plan Management	Initiate QHP Issuer App	SERFF	Provide Issuers with the ability to initiate an application for Issuer certification and be directed to application requirements	Deleted
PM-009	Plan Management	Initiate QHP Issuer App	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 - Issuer Name - license - Solvency - certifications - complaint history - accreditation date - accreditation status	Deleted
PM-010	Plan Management	Initiate QHP Issuer App	SERFF	Provide the ability to receive, store and track the information included in the Notification of Issuer's Intent to Apply	Deleted
PM-011	Plan Management	Initiate QHP Issuer App	Manual	Provide interface/query to state database and/or state License system in order to validate Issuer information	Deleted
PM-012	Plan Management	Initiate QHP Issuer App	Manual	Provide the ability to electronically notify Issuer of validation or non-validation	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-013	Plan Management	Initiate QHP Issuer App	SERFF	Provide the ability to establish and/or verify the existence of an Issuer ID	Validated
PM-014	Plan Management	Initiate QHP Issuer App	Manual	Provide Exchange staff the ability to verify Issuer licensure	Deleted
PM-015	Plan Management	Initiate QHP Issuer App	Manual	Provide the ability to notify the Issuer when an ID has been established	Deleted
PM-016	Plan Management	Initiate QHP Issuer App	SERFF	Allow Issuers to initiate product submissions for approval, for products to be offered on the Exchange	Deleted
PM-017	Plan Management	Initiate QHP Issuer App	SERFF	Allow the issuer to classify applications to indicate Issuer type: licensed to sell outside the Exchange OR licensed to sell on the Exchange	Deleted
PM-018	Plan Management	Initiate QHP Issuer App	SERFF	Allow the issuer to classify applications to indicate Product type: qualified to sell outside Exchange Or on the Exchange Market type: Individual market, small group, large group, Medicaid	Deleted
PM-019	Plan Management	Initiate QHP Issuer App	SERFF	Allow the issuer to classify applications to indicate Exchange Market type: Individual market, small group, large group, Medicaid	Validated
PM-020	Plan Management	Initiate QHP Issuer App	SERFF	Provide the ability to record multiple counties and multiple zip codes by plan to reflect the geographic service area covered by a plan	Deleted
PM-021	Plan Management	Initiate QHP Issuer App	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.)	Validated
PM-022	Plan Management	Initiate QHP Issuer App	SERFF	Provide ability to identify those plans that contain pediatric essential dental benefit	Validated
PM-023	Plan Management	Initiate QHP Issuer App	SERFF	Provide ability to identify those plans that contain pediatric essential vision benefit	Validated
PM-024	Plan Management	Initiate QHP Issuer App	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 direct data entry. This information may include issuer and product plan administrative information, network data, benefit data, rate data, marketing materials, and issuer/product plan attestations.	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-025	Plan Management	Initiate QHP Issuer App	SERFF	Provide the ability to receive data from issuers on at least the following elements: issuer characteristics, product design and rating rules for approval.	Deleted
PM-026	Plan Management	Initiate QHP Issuer App	SERFF	Store information about each plan offered within the Exchange, as required to support plan analysis. Examples of product plan data includes: - Benefits structure/cost sharing requirements - Quality measures and rating data (potentially through existing accreditation entities reporting mechanisms) - Rates - Co-pay and cost sharing information	Validated
PM-027	Plan Management	Establish Issuer and Plan Renewal and Recertification	TBD	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	Deleted
PM-028	Plan Management	Establish Issuer and Plan Renewal and Recertification	Manual	The system must allow the Exchange staff to indicate which plans will be requested to be renewed and which will not.	Deleted
PM-029	Plan Management	Establish Issuer and Plan Renewal and Recertification	Manual	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.	Deleted
PM-030	Plan Management	Establish Issuer and Plan Renewal and Recertification	Manual	The system must be able to receive notifications from Issuers regarding intent to renew or not renew a plan	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-031	Plan Management	Initiate QHP Issuer App	SERFF	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 must support ongoing maintenance through links with the issuers.	Deleted
PM-032	Plan Management	Initiate QHP Issuer App	Manual	Provide the ability to evaluate networks against specific criteria as defined by the Exchange	Deleted
PM-033	Plan Management	Initiate QHP Issuer App	TBD	Provide ability to link consumer queries to Issuer databases and state data sets	Deleted
PM-034	Plan Management	Initiate QHP Issuer App	SERFF	Capture and store Provider Information including: - Provider type - Accepting new patients y/n - Provider demographic information - Provider services information Note: providers can be linked to multiple plans and multiple issuers	Deleted
PM-035	Plan Management	Initiate QHP Issuer App	SERFF	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	Deleted
PM-036	Plan Management	Initiate QHP Issuer App	Manual	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	Deleted
PM-037	Plan Management	Initiate QHP Issuer App	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)	Deferred

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-038	Plan Management	Evaluate QHP Issuer Application	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.	Deleted
PM-039	Plan Management	Evaluate QHP Issuer Application	Manual	Provide the ability via an electronic interface with the appropriate state database resources to validate state insurance licensure, solvency and good standing	Deleted
PM-040	Plan Management	Evaluate QHP Issuer Application	TBD	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	Deleted
PM-041	Plan Management	Evaluate QHP Issuer Application	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).	Deleted
PM-043	Plan Management	Evaluate QHP Issuer Application	SERFF	Provide ability for authorized users to view product information, request supplemental information, update as needed and add additional data to support product evaluation.	Deleted
PM-044	Plan Management	Evaluate QHP Issuer Application	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)	Deleted
PM-045	Plan Management	Evaluate QHP Issuer Application	SERFF	Provide the ability to accommodate time-base criteria to support a defined timeframe for which the criteria is valid	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-046	Plan Management	Evaluate QHP Issuer Application	OneGate	Store historical criteria which is no longer in active use, or has expired for reference	Validated
PM-047	Plan Management	Evaluate QHP Issuer Application	TBD	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.	Deleted
PM-048	Plan Management	Evaluate QHP Issuer Application	SERFF	Provide the ability for Plan Management workers to verify Attestations and supporting documentation	Deleted
PM-049	Plan Management	Evaluate QHP Issuer Application	TBD	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 - Quality, including Accreditation status - Benefit coverage - Cost sharing - Marketing material, etc.	Deleted
PM-050	Plan Management	Evaluate QHP Issuer Application	SERFF	Accommodate variations in criteria by Market (individual, small group, large group).	Validated
PM-051	Plan Management	Evaluate QHP Issuer Application	Manual	Accommodate variations in criteria by Issuer type (Exchange / Non-Exchange).	Deleted
PM-052	Plan Management	Evaluate QHP Issuer Application	Manual	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.	Deleted
PM-054	Plan Management	Evaluate QHP Issuer Application	Manual	Provide the ability to electronically send Notice of Application Status to Issuer	Deleted
PM-055	Plan Management	Evaluate QHP Issuer Application	SERFF	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.	Deleted
PM-056	Plan Management	Evaluate QHP Issuer Application	SERFF	Provide authorized users the ability to enter and store reasons for acceptance or denial of a plan or Issuer into the Exchange	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-057	Plan Management	Evaluate QHP Issuer Application	Manual	Provide the ability to automatically generate formal letter of denial indicating that an Issuer and/or Plan has not been accepted into the Exchange	Deleted
PM-058	Plan Management	Evaluate QHP Issuer Application	Manual	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 (individual or small group) and/or the exchange.	Deleted
PM-059	Plan Management	Rate and Benefit Information Receipt	SERFF	Provide the ability to receive and process Rate and Benefit Data for each product plan offered on the Exchange	Validated
PM-060	Plan Management	Rate and Benefit Information Receipt	Manual	Ability to send notification to Issuers to submit rate and benefit information	Deleted
PM-061	Plan Management	Rate and Benefit Information Receipt	SERFF	Provide Issuers with the ability to provide rate and benefit information in multiple formats including file upload in a format determined by the Exchange, and direct data entry.	Deleted
PM-062	Plan Management	Rate and Benefit Information Receipt	SERFF	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 with cost-sharing requirements associated with the benefit.	Deleted
PM-063	Plan Management	Rate and Benefit Information Receipt	SERFF	Allow Issuers to classify product plans as QHP-applicable and non-QHP-considered; and also classify within a market type (i.e. individual or small group)	Deleted
PM-064	Plan Management	Rate and Benefit Information Receipt	SERFF	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-065	Plan Management	Rate and Benefit Information Receipt	SERFF	Perform data validation on rate/benefit data to ensure accuracy and completeness of supplied data.	Deleted
PM-066	Plan Management	Rate and Benefit Information Receipt	SERFF	Provide electronic notification to Issuers regarding data issues related to rate and benefit information submission(s)	Deleted
PM-067	Plan Management	Rate and Benefit Information Receipt	SERFF	Provide electronic notification to Issuer to provide Final Attestation for Rate/Benefit Data and Information	Deleted
PM-068	Plan Management	Rate and Benefit Information Receipt	SERFF	Allow Insurance Issuers the ability to provide premium information in real-time or as part of the catalog in a batch upload.	Deleted
PM-069	Plan Management	Revise QHP Issuer Application	SERFF	Provide Issuer the ability to withdraw an application for consideration for individual and small group market, and/or consideration in individual exchange and/or SHOP exchange	Deleted
PM-070	Plan Management	Determine Issuer Plan Non-Certification	SERFF	Provide the ability to record the plan non-renewal event and status information, including date, reason/rationale	Deleted
PM-071	Plan Management	Determine Issuer Plan Non-Certification	Manual	Produce electronic and/or paper notices to Issuers when a plan is decertified from Exchange	Deleted
PM-072	Plan Management	Determine Issuer Plan Non-Certification	SERFF	Provide the ability to record the plan or issuer decertification event and status information, including date, reason/rationale	Deleted
PM-073	Plan Management	Determine Issuer Plan Non-Certification	Manual	Produce electronic notification to Insurance Division when a Issuer/plan is not renewed or is decertified from the Exchange	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-074	Plan Management	Determine Issuer Plan Non-Certification	SERFF	Produce electronic notification to CMS when an Issuer/plan is not renewed or is decertified from the Exchange	Deferred
PM-075	Plan Management	Determine Issuer Plan Non-Certification	SERFF	Provide the ability to define an option period for recertification and renewal.	Deleted
PM-076	Plan Management	Determine Issuer Plan Non-Certification	SERFF	Send notification to the Insurance Division or other relevant state agencies of those Issuers and/or Plans which have been denied acceptance to participate in the Exchange.	Deleted
PM-077	Plan Management	Establish QHP Certification and Agreement	SERFF	Provide the ability to open a special certification period to enable certifying an Issuer or Plan outside the defined certification period	Deleted
PM-078	Plan Management	Establish QHP Certification and Agreement	SERFF	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	Deleted
PM-079	Plan Management	Establish QHP Certification and Agreement	Manual	Provide the ability to generate a notification of certification into the Exchange	Deleted
PM-080	Plan Management	Establish QHP Certification and Agreement	SERFF	Allow storage of agreement signature or acceptance date to indicate the Issuer agreement acceptance.	Deleted
PM-081	Plan Management	Establish QHP Certification and Agreement	Manual	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.	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-082	Plan Management	Establish QHP Certification and Agreement	TBD	Determine the quality rating in accordance with CMS plan quality rating methodology.	Deferred
PM-083	Plan Management	Establish QHP Certification and Agreement	SERFF	Display the metal rating of a plan (platinum, gold, silver, bronze)	Validated
PM-084	Plan Management	Establish QHP Certification and Agreement	OneGate	Provide query of plans by issuer with calculated rating for other attributes to be determined by the Exchange.	Deferred
PM-085	Plan Management	Establish QHP Certification and Agreement	OneGate	Provide the ability for plan information to be 'published' to the public exchange view when approval for plan is finalized	Validated
PM-086	Plan Management	Establish QHP Certification and Agreement	OneGate	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 deductible - 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	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-087	Plan Management	Establish QHP Certification and Agreement	OneGate	Provide the ability for plan information to be easily removed from the public exchange view if approval status of the plan changes	Validated
PM-088	Plan Management	Establish QHP Certification and Agreement	Manual	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	Deleted
PM-089	Plan Management	Establish QHP Certification and Agreement	SERFF	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	Deleted
PM-090	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Support receipt of recertification data in the same manner used for initial certification.	Deleted
PM-091	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Support storage, view and processing of recertification data and analysis in the same manner used for initial certification.	Deleted
PM-092	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Distinguish if data and tracking activities are for initial certification or recertification	Deleted
PM-093	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Store and provide the capability to display on demand transactional history related to the QHP certification process, including but not limited to certification/decertification event and rationale for decertification events.	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-094	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Store a record of all QHP negotiation steps, activities, and outcomes.	Deleted
PM-095	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Generate re-amendment notification and information storage consistent with the initial certification amendment process.	Deleted
PM-096	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Process agreement acceptance from Issuers consistent with the initial certification acceptance process	Deleted
PM-097	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Update Issuer and agreement information in the system consistent with the initial certification amendment process.	Deleted
PM-098	Plan Management	Establish Issuer and Plan Renewal and Recertification	Manual/SERFF	Recertify the plan and notify issuers consistent with the initial certification process.	Deleted
PM-099	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	Update CMS with certified plan information consistent with the initial certification process	Validated
PM-100	Plan Management	Establish Issuer and Plan Renewal and Recertification	SERFF	The system must distinguish to CMS initial certified data from recertified plan data.	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-102	Plan Management	Monitor Issuer/Plan Compliance	Manual	Provide the ability to define performance monitoring periods (i.e. quarterly, monthly etc.)	Deferred
PM-103	Plan Management	Monitor Issuer/Plan Compliance	TBD	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 (CAHPS) - Complaints - Patient information programs - Claims payment data - Disenrollment data - Denied claims - Issuer ID - Compliant data/summaries - Sanction data (if any) - Solvency Status - Network Adequacy	Validated
PM-105	Plan Management	Monitor Issuer/Plan Compliance	TBD	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	Deferred
PM-107	Plan Management	Monitor Issuer/Plan Compliance	TBD	Track the receipt of performance and compliance data from Issuers and including date of receipt	Deleted
PM-108	Plan Management	Monitor Issuer/Plan Compliance	TBD	Allow authorized users to track receipt of information received by Issuers in non-data formats, i.e. PDFs	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-109	Plan Management	Monitor Issuer/Plan Compliance	Manual	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	Deferred
PM-110	Plan Management	Monitor Issuer/Plan Compliance	SERFF & OneGate	Indicate the status of an Issuer/Plan compliance determination	Deferred
PM-111	Plan Management	Monitor Issuer/Plan Compliance	SERFF	Allow for preliminary and final compliance determinations	Deferred
PM-112	Plan Management	Monitor Issuer/Plan Compliance	SERFF	Retain historical compliance tracking information	Deferred
PM-113	Plan Management	Monitor Issuer/Plan Compliance	Manual	Provide a compliance dashboard to indicate compliance analysis progress on Issuers/plans and the results of the compliance analysis through the compliance process	Deleted
PM-114	Plan Management	Monitor Issuer/Plan Compliance	TBD	Provide a Performance indicator dashboard to aggregate performance data and display summary performance information by Issuer/Plan	Deleted
PM-115	Plan Management	Monitor Issuer/Plan Compliance	Not for October 2013	Calculate a quality rating for each plan according to a methodology determined by the Exchange.	Deferred
PM-116	Plan Management	Monitor Issuer/Plan Compliance	OneGate	Retain historical plan quality ratings	Deferred

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-117	Plan Management	Monitor Issuer/Plan Compliance	OneGate	Display the most current quality rating for each plan on the consumer website.	Deferred
PM-118	Plan Management	Monitor Issuer/Plan Compliance	Manual	Produce electronic or paper notices for Issuers indicating the results of the compliance and quality reviews, i.e. the compliance and quality rating determination	Deleted
PM-119	Plan Management	Maintain Operational Data	TBD	The system must accept electronic Issuer complaint data in a secure manner, from the Insurance Division on a monthly basis.	Deferred
PM-139	Plan Management	Maintain Operational Data	TBD	Allow Issuers to submit new/changed marketing and Enrollee communication materials	Validated
PM-140	Plan Management	Maintain Operational Data	TBD	Receive electronic files of marketing materials from Issuers	Validated
PM-141	Plan Management	Maintain Operational Data	TBD	Allow users to be able to classify marketing materials from Issuers	Validated
PM-142	Plan Management	Maintain Operational Data	OneGate	Store and track electronic files of marketing materials from Issuers	Validated
PM-143	Plan Management	Maintain Operational Data	OneGate	Allow Plan Management staff to view electronic files of marketing materials	Validated
PM-144	Plan Management	Maintain Operational Data	TBD	Track review and approval activities related to review of marketing materials	Validated
PM-145	Plan Management	Maintain Operational Data	OneGate	Allow Marketing materials to be linked to appropriate plan/issuer records in the system.	Validated
PM-146	Plan Management	Maintain Operational Data	OneGate	Provide capability to categorize marketing materials according to a schema defined by the Exchange	Validated
PM-147	Plan Management	Maintain Operational Data	OneGate	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-148	Plan Management	Maintain Operational Data	TBD	Track marketing material revision requests and the revision process, including tracking data about revision requests such as - Issuer Identifier - Plan Identifier - Marketing Material content - Material review process/tracking information - Revision number	Deferred
PM-149	Plan Management	Maintain Operational Data	TBD	Provide version control document management capabilities for submitted marketing materials in order to manage document submissions and revisions	Validated
PM-150	Plan Management	Maintain Operational Data	TBD	Allow marketing material reviewers to create and send notifications to Issuers about requested revisions	Validated
PM-151	Plan Management	Maintain Operational Data	TBD	Record approval information about marketing materials, including: -Approver -Approve Date -Status	Validated
PM-152	Plan Management	Maintain Operational Data	TBD	Upon approval of marketing materials, generate notification to Issuer regarding approval	Validated
PM-153	Plan Management	Maintain Operational Data	TBD	Upon approval of marketing materials, provide update to Issuer's QHP Account Information	Validated
PM-154	Plan Management	Maintain Operational Data	SERFF	Provide the ability for Issuers to submit Provider Network Information	Validated
PM-155	Plan Management	Maintain Operational Data	OneGate	Provide ability for Exchange staff to view Provider information, update as needed and add additional data not provided electronically.	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-156	Plan Management	Maintain Operational Data	TBD	Accept electronic Provider network information by Issuer from the Insurance Division on a monthly basis. Provider data can include: - Issuer data - Provider data - Provider Contract data - Provider Business data	Duplicate
PM-161	Plan Management	Maintain Operational Data	TBD	Provide the ability for historical Provider data to be saved to provide accurate historical representation of the Provider network at a given point in time	Deleted
PM-162	Plan Management	Maintain Operational Data	Manual	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.	Deferred
PM-163	Plan Management	Maintain Operational Data	Manual	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: - Plan Contact Information - Call Center Information - Addresses - Website Addresses - Management/Key Personnel/Ownership Changes - Plan Name Changes - Banking Information	Deferred
PM-164	Plan Management	Maintain Operational Data	Manual	Notify authorized Exchange users when an Issuer has updated any Issuer, plan and provider data	Deleted
PM-165	Plan Management	Maintain Operational Data	OneGate	Provide the ability for authorized Exchange user to view changes made by a Issuer to Issuer, Plan and Provider data	Deleted
PM-166	Plan Management	Maintain Operational Data	OneGate	Provide ability for an authorized Exchange user to authorize changes made by a Issuer to be posted to the exchange.	Deleted
PM-167	Plan Management	Maintain Operational Data	TBD	Store and track historical Issuer administrative data	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-168	Plan Management	Maintain Operational Data	TBD	Provide ability for Issuers to electronically submit transparency and quality data such as: - Issuer Identifier - Transparency/quality Information: - Payment policies and practices - Financial disclosures - Enrollment/disenrollment data - Claims denials - Rating practices - Quality rating data	Deferred
PM-169	Plan Management	Maintain Operational Data	TBD	Provide the ability to receive electronic documents of transparency or quality information from Issuers	Deferred
PM-171	Plan Management	Maintain Operational Data	TBD	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	Deferred
PM-172	Plan Management	Process Change in Plan Enrollment Availability	Manual	Issuers must be able to electronically communicate a plan enrollment change to the Exchange system. Data required will include: - Enrollment availability status - Rates - Effective dates - Status indicating if new dependent enrollee's are still allowed	Deleted
PM-173	Plan Management	Process Change in Plan Enrollment Availability	Manual	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	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition

PM-174	Plan Management	Process Change in Plan Enrollment Availability	TBD	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
					Validated

PM-176	Plan Management	Process Change in Plan Enrollment Availability	TBD	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.	Validated
PM-177	Plan Management	Process Change in Plan Enrollment Availability	Manual	Upon approval of the enrollment change request, generate an electronic notification to the Insurance Division indicating the plan enrollment status	Deleted
PM-180	Plan Management	Process Change in Plan Enrollment Availability	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 change and other information required by CMS	Validated
PM-182	Plan Management	Process Change in Plan Enrollment Availability	TBD	Allow authorized Navigators/Brokers to manage subscriptions to appropriate Exchange notification functions and features	Validated
PM-183	Plan Management	Issuer Account Mgt	OneGate	The system must allow issuers to create and manage user accounts.	Deleted
PM-184	Plan Management	Issuer Account Mgt	OneGate	Certified issuers shall have the ability to list their QHPs in the Exchange catalog and present information on them.	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-185	Plan Management	Issuer Account Mgt	OneGate	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.	Deleted
PM-186	Plan Management	Issuer Account Mgt	OneGate	Provide the ability for issuer and product information to be "published" to the public exchange view when approval is finalized.	Validated
PM-187	Plan Management	Issuer Account Mgt	OneGate	Provide the ability for issuer and product information to be easily removed from the public exchange view if approval status changes	Validated
PM-188	Plan Management	Issuer Account Mgt	SERFF	The system shall periodically submit data to the appropriate CMS system for plan management and fiscal management functions, as required by federal regulation.	Validated
PM-189	Plan Management	Review Rate Increase Justifications	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	Deleted
PM-190	Plan Management	Review Rate Increase Justifications	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.	Deleted
PM-191	Plan Management	Review Rate Increase Justifications	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.	Deleted
PM-192	Plan Management	Review Rate Increase Justifications	SERFF	Screen submitted rate and benefit data and provide formatting error information back to the Issuer if data format is not correct	Deleted
PM-193	Plan Management	Review Rate Increase Justifications	SERFF	Provide submitted rate and benefit data to the Insurance Division system and CMS electronically	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-194	Plan Management	Review Rate Increase Justifications	SERFF	Provide the ability for authorized users to view and utilize proposed rate and benefit data during the analysis of rate justifications.	Deleted
PM-195	Plan Management	Review Rate Increase Justifications	SERFF	Provide the ability for users to track the steps/progress of rate justification analysis, including steps completed / not completed and dates	Deleted
PM-196	Plan Management	Review Rate Increase Justifications	SERFF	Allow users to track communications with Issuers and Insurance Division to support the analysis/negotiations process	Deleted
PM-197	Plan Management	Review Rate Increase Justifications	SERFF	Provide comparisons between current and proposed rates and plan benefits	Deleted
PM-198	Plan Management	Review Rate Increase Justifications	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.	Deleted
PM-199	Plan Management	Review Rate Increase Justifications	Manual	If a rate increase is denied, generate a denial notice to the issuer both electronically, and as a formal notice that can be mailed.	Deleted
PM-200	Plan Management	Review Rate Increase Justifications	SERFF	Upon approval of rate increase, generate an approval notice to the issuer both electronically, and as a formal notice that can be mailed.	Deleted
PM-201	Plan Management	Review Rate Increase Justifications	Manual	Upon rate increase approval, update certification agreement data and relevant rate and benefit data, effective dates.	Validated
PM-202	Plan Management	Review Rate Increase Justifications	TBD	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.	Deferred
PM-203	Plan Management	Review Rate Increase Justifications	TBD	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 - Plan Identifier - Rate Data - Rating Factors	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-204	Plan Management	Review Rate Increase Justifications	OneGate	Allow the authorized user to publish finalized rates and benefits data to the public facing Exchange.	Validated
PM-205	Plan Management	Revise Rate and Benefit Data	SERFF	Track communications with Issuers and the Insurance Division to support the rate review analysis/negotiation process	Deleted
PM-206	Plan Management	Revise Rate and Benefit Data	Manual	Track if a rate increase denial is being appealed by an Issuer (upon notification by the Issuer).	Deleted
PM-207	Plan Management	Revise Rate and Benefit Data	SERFF	Provide ability for Issuers to re-submit rate and/or benefit information based on Request	Deleted
PM-208	Plan Management	Revise Rate and Benefit Data	SERFF	Perform data validation checks on revised rate and/or benefit data and notify Issuer if additional corrections are required	Deleted
PM-209	Plan Management	Revise Rate and Benefit Data	Manual	Provide a notification to Issuer to submit final Attestation	Deleted
PM-210	Plan Management	Revise Rate and Benefit Data	Manual	Provide Issuers with ability to submit final Attestation	Deleted
PM-211	Plan Management	Revise Rate and Benefit Data	Manual	Capture, store and track Issuer's final Attestation	Deleted
PM-212	Plan Management	Revise Rate and Benefit Data	SERFF	Determine if Issuer provided rate and/or benefit data and information revisions within the designated time-frame	Deleted
PM-213	Plan Management	Revise Rate and Benefit Data	SERFF	Provide electronic and hard-copy notification to Issuer of QHP rate/benefit data and information revision acceptance	Deleted
AD-000	Program Integrity	Retroactive Eligibility Reconciliation	OneGate	Provide the ability to process retroactive eligibility changes including the reconciliation of insurance coverage payments.	Validated
EL-001	Eligibility and Enrollment	General	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).	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-002	Eligibility and Enrollment	Pre-Screening/ Screening	OneGate	Interface with the AHS/DCF 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 AHS/DCF Eligibility System with the option for anonymous screening.	Validated
EL-004	Eligibility and Enrollment	Pre-Screening	OneGate	The Exchange will provide expert-level pre-screening function to Navigators, Brokers, and Exchange Staff	Validated
EL-005	Eligibility and Enrollment	Pre-Screening/ Screening	OneGate	Indicate whether an applicant is already enrolled in a publicly subsidized health coverage program.	Validated
EL-006	Eligibility and Enrollment	Pre-Screening/ Screening	OneGate	Present a more detailed level of screening questions to be addressed at the option of the Individual.	Validated
EL-007	Eligibility and Enrollment	State Subsidy	OneGate	Interface with the AHS/DCF Eligibility System to display eligibility information for VT subsidized public and commercial health plans available through the Exchange.	Validated
EL-008	Eligibility and Enrollment	APTC/CSR	OneGate	Interface with the AHS/DCF Eligibility System to display eligibility information and supporting data for the Advance Premium Tax Credits and Cost Sharing Reductions.	Deleted
EL-009	Eligibility and Enrollment	APTC/CSR	OneGate	Interface with the Federal Exchange Eligibility Service to display eligibility information and supporting data for the Advance Premium Tax Credits and Cost Sharing Reductions.	Validated
EL-010	Eligibility and Enrollment	APTC/CSR	OneGate	Process the Advance Premium Tax Credit and Cost Sharing Reduction amount(s) provided by CMS/IRS and update the individual's account.	Validated
EL-011	Eligibility and Enrollment	APTC/CSR	OneGate	Provide Individuals with the option to accept a lower Advance Premium Tax Credit.	Met
EL-012	Eligibility and Enrollment	APTC/CSR	OneGate	Allow Exchange Staff, Individuals, Brokers, and Navigators to view alerts regarding the need to recalculate the tax credit when needed.	Validated
EL-013	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide the capability for an Individual to identify the source of information used to determine eligibility.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-014	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide individuals with the ability to acknowledge an eligibility determination.	Met
EL-015	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Allow Exchange Staff to submit case information for eligibility determination outside of the standard workflow.	Validated
EL-016	Eligibility and Enrollment	Individual Exemption from Responsibility	OneGate	Send real-time, automated notifications and written notices to Individuals of CMS determinations of exemption status, and update individual accounts accordingly.	Validated
EL-017	Eligibility and Enrollment	Individual Application & Submit Update	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.	Validated
EL-019	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Send notifications to the Individuals, alerting them to submit required eligibility or verification information.	Validated
EL-020	Eligibility and Enrollment	Individual Application & Submit Update	CGI	Send notifications to the Individuals who have not completed their applications informing them of the expiration date.	Validated
EL-021	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Send notifications to the Individuals, Exchange Staff, Brokers, and Navigators of changes to Individuals' applications.	Validated
EL-022	Eligibility and Enrollment	Individual Application & Submit Update	CGI	Send notifications to the Individuals regarding the enrollment process and the status of their application.	Met
EL-023	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	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	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-024	Eligibility and Enrollment	Individual Application & Submit Update	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.	Validated
EL-025	Eligibility and Enrollment	Individual Application & Submit Update	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.	Validated
EL-026	Eligibility and Enrollment	Individual Application & Submit Update	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.	Met
EL-027	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Intake applicant information, including attachments, required to determine eligibility for publically subsidized health coverage programs offered through the Exchange.	Validated
EL-028	Eligibility and Enrollment	Individual Application & Submit Update		Route applicant data, and related attachments, to the AHS/DCF Eligibility System to determine real-time eligibility for publically subsidized programs and commercial health coverage programs offered through the Exchange.	Validated
EL-029	Eligibility and Enrollment	Individual Application & Submit Update	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.	Met
EL-030	Eligibility and Enrollment	Individual Application & Submit Update	N/A	Route eligibility related attachments from users to Medicaid/CHIP to support eligibility processing and determination.	Validated
EL-031	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide the capability to identify Navigators and Brokers if they are completing applications on behalf of an Individual.	Validated
EL-032	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide the capability for the Individual to attest that any information provided by a Navigator or Brokers is accurate.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-033	Eligibility and Enrollment	Pre-Screening/ Screening	OneGate	Interface with the AHS/DCF Eligibility System to provide Individuals and authorized representatives with the option to complete pre-screening for eligibility for Federal health plans through a real-time interface with the Federal Exchange Eligibility Service with the option for anonymous screening.	Deleted
EL-034	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Display an Individual's eligibility and subsidies under all tiers of QHP benefits through an interface with the AHS/DCF Eligibility System.	Validated
EL-035	Eligibility and Enrollment	Individual Exemption from Responsibility	OneGate	Provide the capability for an Individual to indicate various types of potential exemptions through the single, integrated application process.	Validated
EL-036	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Process documents received in the mail, via facsimile, web portal, and/or email.	Validated
EL-037	Eligibility and Enrollment	Native Americans	OneGate	Allow qualified Native Americans to switch plans on a monthly basis.	Validated
EL-038	Eligibility and Enrollment	Native Americans	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.	Validated
EL-039	Eligibility and Enrollment	Native Americans	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.	Met
EL-040	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide the capability to adjust the calculation of MAGI with allowed exclusions for qualified Native Americans per the ACA regulations.	Validated
EL-041	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Distribute and collect, through a range of mediums, individual, employer, and employee enrollment forms.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-042	Eligibility and Enrollment	Individual Application & Submit Update	N/A	Provide an indicator for individuals determined eligible for Medicaid and CHIP who access coverage through the Exchange	Met
EL-043	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Ask knowledge-based ID questions based on data gathered from external data sources to facilitate authentication of identity.	Validated
EL-044	Eligibility and Enrollment	Individual Eligibility Determination-Verification	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.	Validated
EL-045	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Validate Individual application information for completeness of data and prompt the Individual for additional information, if applicable.	Met
EL-046	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Provide the capability to gather and display Individual and household eligibility data from external sources.	Validated
EL-047	Eligibility and Enrollment	Individual Application & Submit Update	Locate	Validate mailing addresses provided in applications (using an external Postal Address validation service).	Deferred
EL-048	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Allow for a manual verification process when the federal hub verification service is not available through the business rules engine.	Duplicate
EL-049	Eligibility and Enrollment	Individual Eligibility Determination-Verification	Siebel Public Sector CRM	Support a dispute process.	Validated
EL-050	Eligibility and Enrollment	Individual Eligib	OneGate	Provide capability to manually update incarceration status based documentation provided by the Individual (e.g. release papers).	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-051	Eligibility and Enrollment	Participation in the Exchange	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.	Validated
EL-052	Eligibility and Enrollment	Participation in the Exchange	~~OneGate~~	Update individual accounts with the verification results as appropriate.	Met
EL-053	Eligibility and Enrollment	Income Verification	OneGate	Provide the capability for an Individual to confirm income data from external sources.	Met
EL-054	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Provide the ability to verify information needed to evaluate eligibility for VT subsidized health plans.	Validated
EL-055	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Provide the ability for Individuals to submit images of documents required for eligibility verification.	Met
EL-056	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Generate online or written requests to Individuals for additional documentation of annual / monthly income, allow electronic submission of documents, link to accounts, and track follow up activities.	Validated
EL-057	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Allow Exchange Staff, Brokers, and Navigators to view, save, and print Individual verification documents that have been up-loaded to a case.	Met
EL-058	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Provide the capability to allow designated users to confirm, notate and mark active/non-active status of verification documents and verification results.	Met
EL-059	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Allow Exchange Staff, Individuals, Brokers, and Navigators to provide alternative verification through multiple methods.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall…"	Current Disposition
EL-060	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Provide the ability to allow Individuals to view, confirm, dispute and submit corrections to verification results.	Met
EL-061	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Support checks for Medicaid eligibility that can not be serviced real-time. Responses should be accepted later, and user shall be permitted to negotiate enrollment in a QHP while waiting for a response.	Validated
EL-062	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Provide the capability to accept notifications from Medicaid/CHIP regarding loss of coverage, and should evaluate those individuals for QHP subsidized coverage.	Validated
EL-063	Eligibility and Enrollment	Participation in the Exchange	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.)	Validated
EL-064	Eligibility and Enrollment	Individual Eligibility Determination-Verification	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.	Validated
EL-065	Eligibility and Enrollment	Change Management	N/A	Provide the ability to update information related to other components of eligibility not described above, including access to minimum essential coverage.	Validated
EL-066	Eligibility and Enrollment	Change Management	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.	Met
EL-067	Eligibility and Enrollment	Change Management	OneGate	Provide consumers the ability to view the new determination of eligibility after the change in circumstances.	Met
EL-068	Eligibility and Enrollment	Change Management	OneGate	Provide users the ability to choose new health plans after the re-determination process based on the new circumstances.	Met
EL-069	Eligibility and Enrollment	Case Inquiry	OneGate	Allow Exchange Staff, customers, call center staff and Navigators to search for a customer's household information and composition.	Met
EL-070	Eligibility and Enrollment	Case Inquiry	OneGate	Allow Exchange Staff, customers, call center staff and Navigators to view a customer's household information and composition.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-071	Eligibility and Enrollment	Case Inquiry	OneGate	Allow Exchange Staff, customers, call center staff and Navigators to add, update, modify and delete household composition information.	Validated
EL-072	Eligibility and Enrollment	Identity Management	Oracle MDM (Customer Hub)	Provide automatic checks for duplicate household members within other cases in the system.	Validated
EL-073	Eligibility and Enrollment	Identity Management	OneGate	Allow Exchange Staff, call center staff and Navigators to merge or associate different household members together.	Validated
EL-074	Eligibility and Enrollment	Identity Management	OneGate	Provide the ability to split family relationships and to assign certain field information to the appropriate people.	Validated
EL-33	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Allow continuance of the application process for Individuals without an SSN (e.g. newborns and undocumented Individuals).	Met
ELM-001	Eligibility and Enrollment	Pre-Screening	OneGate	Provide the option for anonymous completion of MAGI eligibility related questions	Validated
ELM-002	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	Validated
ELM-003	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).	Deleted
ELM-004	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).	Validated
ELM-005	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).	Met
ELM-006	Eligibility and Enrollment	Income Verification	OneGate	As part of the application process, collect household and income information to determine if the household is under 100% FPL.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
ELM-007	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).	Met
ELM-008	Eligibility and Enrollment	Change Management	OneGate	Store changed information along with the date the information was changed.	Validated
ELM-009	Eligibility and Enrollment	Change Management	OneGate	Support prompting users / consumers to renew their application on an annual basis.	Validated
ELM-010	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.	Validated
ELM-011	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide a method to identify persons who are eligible for services.	Met
ELM-012	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.	Validated
ELM-013	Eligibility and Enrollment	Individual Application & Submit Update	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.	Met
ELM-014	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).	Validated
ELM-015	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).	Validated
ELM-016	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). .	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
ELM-017	Eligibility and Enrollment	Individual Application & Submit Update	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.	Met
ELM-018	Eligibility and Enrollment	Application Process	OneGate	Identify and display verifications required for the applicant based on program rules.	Validated
ELM-019	Eligibility and Enrollment	Application Process	OneGate	Produce a customized listing of verification documents for an eligibility criteria required to complete eligibility determination.	Met
ELM-021	Eligibility and Enrollment	Application Process	OneGate	Present the applicant with a summary view of the information entered prior to submission.	Met
ELM-022	Eligibility and Enrollment	Application Process	OneGate	Allow applicants to print /save a copy of electronic copy for their records.	Validated
ELM-023	Eligibility and Enrollment	Application Process	OneGate	Allow an applicant or applicant's authorized representative to review the current application before and after formal submission.	Validated
ELM-024	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.	Validated
ELM-025	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.	Validated
ELM-026	Eligibility and Enrollment	Application Process	OneGate	Allow and record an applicant's request to withdraw an application.	Deferred
ELM-027	Eligibility and Enrollment	Application Process	CGI	Collect and manage information about beneficiary population from diverse sources.	Validated
ELM-028	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Provide an automated or guided application process to enable the applicant/worker to easily enter required information.	Met
ELM-029	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.	Validated
ELM-030	Eligibility and Enrollment	Application Process	CGI	Provide system-generated date and time stamp for registration of paper applications.	Validated
ELM-031	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to begin benefits on a date different than the application date and system-generated date.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
ELM-032	Eligibility and Enrollment	Application Process	OneGate	Capture and display date that a disposition was made on an application/renewal.	Validated
ELM-033	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.	Duplicate
ELM-034	Eligibility and Enrollment	Application Process	OneGate	Route applications to the appropriate staff, based on business rules.	Validated
ELM-035	Eligibility and Enrollment	Application Process		Display to the applicant discrepant information between the new application and information stored in the existing household.	Validated
ELM-036	Eligibility and Enrollment	Application Process	OneGate	Allow for a manual verification process when the Federal or State hub verification service is not available.	Validated
ELM-037	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to indicate which verification documents have already been provided.	Met
ELM-038	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).	Validated
ELM-039	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to manually extend verification timeframes.	Validated
ELM-040	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to track required verification timeframes.	Validated
ELM-041	Eligibility and Enrollment	Application Process	OneGate	Provide a mechanism to generate a list of received and pending verifications including eligibility worker entered comments.	Met
ELM-042	Eligibility and Enrollment	Application Process	OneGate	Provide the ability to allow applicants to view, confirm, dispute and submit corrections to verification results.	Validated
ELM-043	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.	Validated
ELM-044	Eligibility and Enrollment	Application Process	OneGate	Update the applicant's record with the verification results as appropriate.	Met
ELM-045	Eligibility and Enrollment	Application Process	OneGate	Assure consistency in eligibility determination processing when applicants attempt to access services through different entry points.	Met
ELM-046	Eligibility and Enrollment	Application Process	OneGate	Provide the capability to determine and correct eligibility for current and prior months.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
ELM-047	Eligibility and Enrollment	Application Process	OneGate	Display the eligibility results in a manner that is comprehensive and easy to understand.	Met
ELM-048	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.	Met
ELM-049	Eligibility and Enrollment	Household Maintenance	tbd	Auto-populate known data within the system between modules and functions within the life of the household.	Validated
ELM-050	Eligibility and Enrollment	Household Maintenance	tbd	Provide a mechanism to edit and store certain automatically populated data as defined by the State.	Validated
ELM-051	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.	Met
ELM-052	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism for authorized users to access beneficiary/household summary from any screen.	Validated
ELM-053	Eligibility and Enrollment	Household Maintenance	OneGate	Provide the functionality to reinstate service coverage until the Administrative Appeals decision is rendered.	Validated
ELM-054	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.	Validated
ELM-055	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism to indicate relationships between all members of a household.	Met
ELM-057	Eligibility and Enrollment	Household Maintenance	CGI	Provide the capability to perform mass terminations due to changes in status as well as program changes.	Validated
ELM-058	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism to indicate that a beneficiary/household is under review.	Validated
ELM-059	Eligibility and Enrollment	Household Maintenance	OneGate	Provide a mechanism to alert management that pending applications have exceeded specified time limits.	Validated
ELM-060	Eligibility and Enrollment	Household Maintenance	OneGate	Automatically create an alert of approaching deadlines.	Validated
ELM-061	Eligibility and Enrollment	Household Maintenance	OneGate	Allow applicant/beneficiaries to self-report changes in their personal information online, described by the State when changes are made.	Met
ELM-062	Eligibility and Enrollment	Household Maintenance	OneGate	Provide the capability to view the new determination of eligibility after the change in information.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
ELM-063	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.	Validated
ELM-064	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.	Validated
ELM-065	Eligibility and Enrollment	Household Maintenance	Audit Logging	Provide the capability to track and record any changes to an individual's information.	Validated
ELM-066	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.	Met
ELM-067	Eligibility and Enrollment	Household Maintenance	OneGate	Change the status of any individual in a household without terminating eligible household members.	Validated
ELM-068	Eligibility and Enrollment	Household Maintenance	OneGate	Provide web-based functionality to allow the applicant to renew eligibility online.	Validated
ELM-069	Eligibility and Enrollment	Household Maintenance	CGI	Allow for renewals that do not occur online.	Validated
ELM-070	Eligibility and Enrollment	Household Maintenance	OneGate	Track when a renewal is due.	Validated
ELM-071	Eligibility and Enrollment	Household Maintenance	OneGate + CGI noticing	Have the ability to track which renewals have been sent and which have been returned.	Validated
ELM-072	Eligibility and Enrollment	Household Maintenance	OneGate + CGI noticing	Have the ability to automatically send renewal notices to beneficiaries	Validated
ELM-073	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.	Validated
ELM-074	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). .	Validated
ELM-075	Eligibility and Enrollment	Household Maintenance	OneGate	Recalculate and redetermine eligibility when a change in circumstance occurs (e.g., household composition changes, child turning 19).	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
ELM-076	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.	Validated
ELM-077	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.	Validated
ELM-078	Eligibility and Enrollment	Household Maintenance	OneGate	Assure renewal forms meet the same accessibility standards as application.	Validated
ELM-079	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).	Validated
ELM-080	Eligibility and Enrollment	Workflow Management	OneGate	Support both task-based and household-based operations.	Met
ELM-081	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.	Met
ELM-082	Eligibility and Enrollment	Workflow Management	OneGate	Track, monitor, and display work done/ in queue to supervisors.	Validated
ELM-083	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.	Met
ELM-084	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.	Validated
ELM-085	Eligibility and Enrollment	Interfaces	CGI	Alert eligibility workers or a processing queue when beneficiary information is updated through an automated interface.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
ELM-086	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.	Validated
ELM-087	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.	Validated
ELM-20	Eligibility and Enrollment	Application Process	OneGate	Allow the worker/applicant to upload and attach source documents to support eligibility determination.	Met
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.).	Validated
EN-001	Eligibility and Enrollment	Plan Selection	OneGate	Prepare an enrollment questionnaire to gather individual preferences and help refine choices of plan to be displayed.	Validated
EN-002	Eligibility and Enrollment	Plan Selection	OneGate	Store enrollment questionnaire responses and display plan choices based on questionnaire / filtering criteria.	Met
EN-003	Eligibility and Enrollment	Plan Selection	OneGate	Based on issuer and plan information gathered, display plan cost and availability.	Met
EN-004	Eligibility and Enrollment	Plan Selection	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.	Met
EN-005	Eligibility and Enrollment	Plan Selection	OneGate	Display actual plan cost based on applicable rating factors (individuals covered, age, geography, etc.) provided by the individual during the application process.	Met
EN-006	Eligibility and Enrollment	Plan Selection	OneGate	If applicable, display an adjusted plan cost based on reduced cost sharing or tax credit advance eligibility.	Met
EN-007	Eligibility and Enrollment	Plan Selection	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.	Duplicate
EN-009	Eligibility and Enrollment	Plan Selection	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.	Validated
EN-010	Eligibility and Enrollment	Plan Selection	OneGate	Provide capability to display a detailed comparison of available health plans based on individual preferences.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EN-011	Eligibility and Enrollment	Plan Selection	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.	Met
EN-012	Eligibility and Enrollment	Plan Selection	OneGate	Provide hyperlinks to Issuer/Plan sites for individuals to obtain further information from Issuers	Met
EN-013	Eligibility and Enrollment	Plan Selection	OneGate	Provide capability for an individual to select a QHP and initiate the enrollment process.	Validated
EN-014	Eligibility and Enrollment	Plan Selection	OneGate	Prevent individuals that have a current QHP selection pending from adding a new QHP or changing their pending selection.	Validated
EN-015	Eligibility and Enrollment	Plan Selection	OneGate	Once a plan is selected, direct an individual to issuer-specific specific instructions on payment remittance for monthly premiums.	Validated
EN-015	Eligibility and Enrollment	Plan Selection	OneGate	Once a plan is selected, direct an individual to issuer-specific specific instructions on payment remittance for monthly premiums.	Validated
EN-016	Eligibility and Enrollment	Plan Selection	OneGate	Update an individuals account to reflect plan selection and the effective plan-year.	Met
EN-017	Eligibility and Enrollment	Plan Selection	OneGate/CGI	After plan selection, initiate the plan enrollment process / electronic transaction to applicable issuers.	Validated
EN-018	Eligibility and Enrollment	Plan Selection	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.	Deleted
EN-019	Eligibility and Enrollment	Enrollment	OneGate	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.	Validated
EN-020	Eligibility and Enrollment	Enrollment	OneGate	Record and store current plan enrollment information for all individuals registered on the Exchange.	Met
EN-021	Eligibility and Enrollment	Enrollment	OneGate/CGI	Process in real-time, the electronic confirmation / acknowledgement of receipt of enrollment transaction from issuer.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EN-022	Eligibility and Enrollment	Enrollment	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.	Validated
EN-023	Eligibility and Enrollment	Enrollment	Healthation	Prepare and electronic, real-time electronic 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 renew his or her enrollment in the qualified health plan.	Validated
EN-025	Eligibility and Enrollment	Enrollment	OneGate	Provide capability to receive electronic notifications from issuers regarding disenrollment and initiate disenrollment process	Validated
EN-025	Eligibility and Enrollment	Enrollment	OneGate	Provide capability to receive electronic notifications from issuers regarding disenrollment and initiate disenrollment process	Validated
EN-026	Eligibility and Enrollment	Enrollment	OneGate	Provide the capability for an individual to request a voluntary disenrollment from a QHP.	Validated
EN-027	Eligibility and Enrollment	Enrollment	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.	Validated
EN-028	Eligibility and Enrollment	Enrollment	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.	Validated
EN-028	Eligibility and Enrollment	Enrollment	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.	Validated
EN-029	Eligibility and Enrollment	Enrollment	OneGate	Update user accounts based on disenrollment notification from issuers or disenrollments initiated by the Exchange.	Validated
EN-030	Eligibility and Enrollment	Enrollment	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.	Validated
EN-030	Eligibility and Enrollment	Enrollment	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EN-031	Eligibility and Enrollment	Enrollment	OneGate	When a plan is decertified, initiate the health plan enrollment process for affected individuals (based on special enrollment period rules).	Validated
EN-032	Eligibility and Enrollment	Enrollment	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.	Validated
EN-033	Eligibility and Enrollment	Enrollment	OneGate	Prepare and provide communication to individuals about a mid-year plan decertification and notify need for plan selection / enrollment.	Duplicate
EN-035	Eligibility and Enrollment	Enrollment	OneGate	Prepare on-screen notification to individuals regarding eligibility for enrollment periods.	Validated
EN-036	Eligibility and Enrollment	Periodic Reporting	Oracle BI	Periodically and on an ad hoc basis provide electronic report to issuers about individual QHP enrollment data	Validated
EN-037	Eligibility and Enrollment	Periodic Reporting	Premium Processor / One Gate	Automatically identify and process issuer discrepancies and payment information	Validated
EN-038	Eligibility and Enrollment	Periodic Reporting	Oracle BI	Generate report of periodic issuer reconciliation to CMS	Validated
EN-039	Eligibility and Enrollment	Periodic Reporting	OneGate	Generate annual report to individual about QHP enrollment	Deferred
EN-040	Eligibility and Enrollment	Periodic Reporting	Oracle BI	Generate annual report to IRS about QHP enrollment	Deferred
MO-023	Enrollment	Medicaid Plan Enrollment	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)	Validated
MO-025	Enrollment	Medicaid Plan Enrollment	OneGate	Provide a mechanism to determine plan assignment, defined by the DHS, if an individual fails to select a plan within the required timeframe.	Validated
MO-026	Enrollment	Medicaid Plan Enrollment	OneGate	Allow for retroactive plan enrollment based on criteria established by DHS.	Validated
MO-027	Enrollment	Medicaid Plan Enrollment	OneGate	Transmit plan selection electronically based on DHS defined criteria.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
MO-24	Medicaid Plan Enrollment	Plan Selection	OneGate	Allow Medicaid-eligible individuals to view available plans in the plan selection module with the same level of functionality offered to individuals shopping in the commercial market	Met
WP-026	Web Portal	Pre-Screening/ Screening	OneGate	Provide calculator functionality for individuals to estimate their premiums including potential premium tax credit subsidies and cost sharing reductions	Duplicate
WP-033	Web Portal	Enrollment	OneGate	Enable individual users to enroll in a plan which they have selected	Duplicate
WP-035	Web Portal	Financial Management	OneGate	Allow users to set up payment options for their selected plan(s)	Duplicate
WP-036	Web Portal	Financial Management	OneGate	Allow users to make recurring and scheduled electronic premium payments through the Exchange portal	Duplicate
SH-001	Small Business	Prepare Employer Application	OneGate	Provide field level help for each preliminary questionnaire and application data element that includes description and required data format.	Met
SH-002	Small Business	Prepare Employer Application	OneGate	Provide capability for employers to access in-depth online help during the preliminary questionnaire process; provide the tools to educate Employers on the services provided within the Exchange.	Validated
SH-003	Small Business	Prepare Employer Application	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.	Deferred
SH-004	Small Business	Prepare Employer Application	OneGate	Provide multiple methods for an employer to build an employee roster through the application process (e.g. manual entry, file upload, etc.)	Met
SH-005	Small Business	Plan Selection/ Employer Application	OneGate	Generate a request to initiate the employer selection of qualified health plan during the application process.	Met
SH-006	Small Business	Plan Selection	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.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-007	Small Business	Plan Selection	OneGate	Based on carrier and plan information gathered, display plan cost and availability based on initial questionnaire completed by the employer.	Validated
SH-008	Small Business	Plan Selection	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.	Deleted
SH-009	Small Business	Plan Selection	OneGate	Display actual plan cost based on applicable rating factors (consumers covered, age, geography, etc.) provided by the employer during the application process.	Deleted
SH-010	Small Business	Plan Selection	OneGate	Provide capability to display a detailed comparison of available health plans based on employer preferences, including product categories.	Deleted
SH-011	Small Business	Plan Selection	OneGate	Provide capability to display a detailed and cost comparison of all available health plans based on information about employees and employee dependents listed in the employee roster.	Validated
SH-012	Small Business	Plan Selection	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 choices, and the ability to view all available plans based on a specified tier.	Deferred
SH-013	Small Business	Plan Selection	OneGate	Provide capability for an employer to select QHP(s), or a tier, and initiate the participation process.	Deleted
SH-014	Small Business	Plan Selection	OneGate	Provide functionality to have a small business tax calculator available to small employers.	Met
SH-015	Small Business	Plan Selection	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.	Validated
SH-016	Small Business	Plan Selection	OneGate	If applicable, display an adjusted plan final cost based on an estimated small business tax credit eligibility as determined by federal data hub interface, 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 expected with the small business tax credit.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-017	Small Business	Plan Selection	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 and display language pertaining to legal implications of eligibility determination to the employer.	Validated
SH-018	Small Business	Plan Selection	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.	Met
SH-019	Small Business	Employer/Employee Application	OneGate	Provide capability to accept paper documents for SHOP, such as employer / employee applications and verifications.	Validated
SH-020	Small Business	Employer Application	OneGate	Allow authorized assistors to complete employer applications on behalf of the employer (i.e. an administration or finance department/personnel, etc.)	Validated
SH-021	Small Business	Employer Application	OneGate	Provide a single, online employer application for Small Business	Met
SH-022	Small Business	Employer Application	OneGate	During the Application Process, prompt the Employer to enter the exact business name associated with the EIN.	Validated
SH-023	Small Business	Employer Application	OneGate	Provide the capability to differentiate / track full-time employees versus part-time/hourly employees in the employee roster.	Met
SH-024	Small Business	Employer Application	OneGate	Validate field-level information for correct data format and completeness	Met
SH-025	Small Business	Employer Application	Loqate	Conduct validation of mailing addresses provided in applications (using external Postal Address validation service)	Deferred
SH-026	Small Business	Employer Application	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 suspension of eligibility if EIN remains un-verified.	Validated
SH-027	Small Business	Employer/Employee Application	OneGate	Within the employer and employee application, the Exchange shall validate field-level information for format and completeness	Met
SH-028	Small Business	Employer Application	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.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-029	Small Business	Employer Application	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)	Validated
SH-030	Small Business	Employer Application	OneGate	Provide capability to validate employee SSNs and TINs submitted through the employer application (employee roster).	Validated
SH-031	Small Business	Employer Application	Oracle Identity Manager	Create user name and password for each employee listed on employee roster.	Deleted
SH-032	Small Business	Employer Application	OneGate	Allow employer-authorized broker/assister to submit all or select data for Employer Application	Validated
SH-033	Small Business	Employer Application	OneGate	Capture broker/assister of record in the employer and account information	Validated
SH-034	Small Business	Employer/Employee Application	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 Exchange should check for an existing unique identifier / account. If one does not exist, the Exchange will facilitate the creation of a new unique identifier.	Validated
SH-035	Small Business	Employer/Employee Application	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 Tax Credit (For Profit or Tax Exempt), SHOP Eligibility)	Validated
SH-036	Small Business	Employer/Employee Application	OneGate	Support the creation of a user account for both employers and employees that defines a user-defined, user name and password.	Met
SH-037	Small Business	Plan Selection	OneGate	Update an employer's account to reflect plan selection and the effective projected plan-year.	Met
SH-038	Small Business	Communicate Options to Employees	OneGate	Provide the capability for the employer to generate a packet of critical information to distribute to the employee.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-039	Small Business	Communicate Options to Employees	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 employee about the open enrollment period and SHOP website access.	Met
SH-040	Small Business	Verify Employer Data on Eligibility Application	OneGate	Provide capability to generate a request to the VT DOL to verify an employer's size.	Deferred
SH-041	Small Business	Verify Employer Data on Eligibility Application	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.)	Deferred
SH-042	Small Business	Verify Employer Data on Eligibility Application	OneGate	Display the result of the verification provided by Department of Labor; provide means for an employer to dispute, call into question or appeal the validity of data from authoritative sources	Validated
SH-043	Small Business	Verify Employer Data on Eligibility Application	OneGate	Provide capability to electronically store documents submitted for verification of employer size, business address, coverage, and number of full-time employees.	Deferred
SH-044	Small Business	Verify Employer Data on Eligibility Application	OneGate	Track status of employer size verification based on the following: - Verified - Not verified - Pending Review	Deferred

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-045	Small Business	Verify Employer Data on Eligibility Application	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, potentially - Employer EIN - Information requested - Due date based on date of initial application	Validated
SH-046	Small Business	Verify Employer Data on Eligibility Application	OneGate	When additional verification is required, provide on-screen notification to employer to supply additional verifications through the Exchange.	Deferred
SH-047	Small Business	Verify Employer Data on Eligibility Application	OneGate	Update user / employer account status based on updated results for employer size, business address, coverage and number of full time employees	Validated
SH-048	Small Business	Verify Employer Data on Eligibility Application	OneGate	Provide capability to generate a request to the Information Source To Be Determined (TBD) to verify Business Address or Worksite.	Deferred
SH-049	Small Business	Verify Employer Data on Eligibility Application	OneGate	Provide the capability to initiate a manual verification process when additional verification of Business Address or Worksite is required.	Deferred
SH-050	Small Business	Verify Employer Data on Eligibility Application	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	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-051	Small Business	Verify Employer Data on Eligibility Application	OneGate	Provide capability to electronically store documents submitted for Business Address or Worksite verification.	Validated
SH-052	Small Business	Verify Employer Data on Eligibility Application	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	Validated
SH-053	Small Business	Verify Employer Data on Eligibility Application	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 - Employer EIN - Information requested - Due date based on date of initial application	Duplicate
SH-054	Small Business	Verify Employer Data on Eligibility Application	OneGate	When additional verification is required, provide on-screen notification to employer to supply additional verifications through the Exchange.	Validated
SH-055	Small Business	Verify Employer Data on Eligibility Application	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.	Validated
SH-056	Small Business	Verify Employer Data on Eligibility Application	OneGate	Provide the capability to initiate a manual verification process when additional verification of Coverage Offered to all Full Time Employed Employees is required.	Deferred

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-057	Small Business	Determine Employer Eligibility	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.	Validated
SH-058	Small Business	Determine Employer Eligibility	OneGate	Generate a request to determine whether an employer meets size, location and employee coverage requirements to utilize the Small Business Exchange	Met
SH-059	Small Business	Determine Employer Eligibility	OneGate	Conduct an eligibility determination as to whether an employer meets size, location and employee coverage requirements to utilize the Small Business Exchange	Met
SH-060	Small Business	Determine Employer Eligibility	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.	Deleted
SH-061	Small Business	Determine Employer Eligibility	OneGate	Generate written and on-screen notification of the result of an employer's eligibility determination	Validated
SH-062	Small Business	Plan Selection	OneGate	Allow the Exchange to set different start dates and waiting periods for different QHPs and employers	Validated
SH-063	Small Business	Plan Selection	OneGate	Prevent employers that have current QHP selection(s) pending from adding new QHP(s) or changing their pending selection.	Met
SH-064	Small Business	Plan Selection / Employee Enrollment	OneGate	After plan selection by the employees and the employer has submitted payment, initiate the plan enrollment process / transaction to applicable carriers.	Validated
SH-065	Small Business	Employer Contribution	OneGate	Provide the capability to determine participation rates of an employer's employees. Provide the capability to share this information with issuers.	Met
SH-066	Small Business	Employer Contribution	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.	Validated
SH-067	Small Business	Employer Contribution	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-068	Small Business	Employer Contribution	OneGate	When plan costs to the employer are finalized, the Small Business Exchange shall provide the flexibility for the Employer to review and compare employer choice models.	Met
SH-069	Small Business	Employer Contribution	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	Met
SH-070	Small Business	Employer Contribution	OneGate	Provide decision support tools, including an online calculator that supports 'what if' scenarios	Validated
SH-071	Small Business	Employer Contribution	OneGate	Recognize future coverage, and manage the effective date based on future coverage information	Validated
SH-072	Small Business	Employer Contribution	OneGate	Allow employer contribution to be based on multiple employee choice models, including choice within a tier, choice of carrier or entire exchange, or full employee choice	Validated
SH-073	Small Business	Employer Contribution	OneGate	Allow employers to provide a contribution for employees to select a plan on the Individual Exchange	Deleted
SH-074	Small Business	Employer Contribution	OneGate	Allow employers to use wage information to compare coverage options to alternatives available to their employees in the Individual Exchange	Validated
SH-075	Small Business	Plan Selection / Employee Enrollment	OneGate	Upon acceptance of final offer from carrier to employer and collection of 1st month's premium payment, generate enrollment transaction to a carrier.	Validated
SH-076	Small Business	Employer / Employee Termination	OneGate	Provide capability to provide termination notices in multiple forms, including in email and paper form.	Validated
SH-077	Small Business	Employer / Employee Termination	OneGate	Allow SHOP Employers to identify/manage the employees within the Exchange	Validated
SH-078	Small Business	Employer Termination	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-079	Small Business	Employer Termination	OneGate	Provide capability to administer COBRA/VIPER, supporting these enrollments and disenrollments.	Validated
SH-080	Small Business	Employer Termination	OneGate	Provide the capability for an employer to request a voluntary termination from QHP(s) at any time.	Validated
SH-081	Small Business	Employer / Employee Termination	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 protections as defined by the Exchange.	Validated
SH-082	Small Business	Employer Termination	OneGate	If an employer initiates a voluntary termination, produce an electronic notification to the Issuer to terminate the employer.	Validated
SH-083	Small Business	Employer Termination	OneGate	If conditions for a voluntary termination, initiate the employer termination process.	Validated
SH-084	Small Business	Employer Termination	OneGate	Provide the capability to image and store documents sent to the employer regarding the employer's termination.	Validated
SH-085	Small Business	Employer / Employee Termination	OneGate	Update user accounts based on termination notification from issuers or terminations initiated by the Exchange.	Validated
SH-086	Small Business	Employer Termination	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., as applicable.	Validated
SH-087	Small Business	Employer Termination	OneGate	Provide capability to receive electronic notifications from issuers regarding involuntary terminations and initiate termination process.	Validated
SH-088	Small Business	Employer Termination	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.	Validated
SH-089	Small Business	Employer Termination	3rd Party Premium Processor	Provide capability to produce two different notifications to employees during a involuntary employer termination, regarding the potential or actual termination of an employer.	Deleted
SH-090	Small Business	Employer Termination	OneGate	If conditions for an involuntary termination are present, initiate the termination process.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-091	Small Business	Employer Termination	3rd Party Premium Processor	If an employer has an involuntary termination through the Exchange, prepare communication to the Issuer to terminate the employer.	Validated
SH-092	Small Business	Employer Termination	OneGate	Update user accounts based on termination notification from issuers or terminations initiated by the Exchange.	Validated
SH-093	Small Business	Employer Termination	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.	Validated
SH-094	Small Business	Employer Termination	OneGate	Notify QHPs when an employer terminates coverage and ensure coverage is discontinued	Validated
SH-095	Small Business	Employer Termination	OneGate	Notify employees when an employer terminates coverage and ensure coverage is discontinued. Employees must be given a 30 day notice of termination.	Validated
SH-096	Small Business	Renewal	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.	Deferred
SH-097	Small Business	Renewal	OneGate	Process employer responses to renew eligibility and initiate eligibility determination process if necessary.	Deferred
SH-098	Small Business	Renewal	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.	Deferred
SH-099	Small Business	Employer Renewal	OneGate	Based on the availability of QHP(s), determine availability of an employer's current plan for the purposes of participation renewal.	Validated
SH-100	Small Business	Employer Renewal	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.	Deferred
SH-101	Small Business	Update Employer Eligibility Application	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 through the Exchange.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-102	Small Business	Renewal, Employee Enrollment	OneGate	Based on an employer's responses to enrollment renewal, assess responses for need to initiate enrollment into a new QHP or additional employees into an existing QHP.	Validated
SH-103	Small Business	Renewal, Employee Enrollment	OneGate	Based on an employer's responses to enrollment renewal, process enrollment selections if possible.	Deleted
SH-104	Small Business	Renewal, Employee Enrollment	OneGate	Process notification notifying employer of coverage for employees. Also, communicate any next steps required by the employer.	Validated
SH-105	Small Business	Employer Renewal	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.	Validated
SH-106	Small Business	Update Employer Eligibility Application	OneGate	Based on employer status, determine eligibility for SHOP participation renewal (e.g. annual renewal).	Validated
SH-107	Small Business	Update Employer Eligibility Application	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.	Validated
SH-108	Small Business	Employer Renewal	OneGate	Produce a notice of annual open enrollment.	Validated
SH-109	Small Business	Employer Renewal	OneGate	Present opportunity for employer to log-in to initiate their renewal.	Validated
SH-110	Small Business	Appeal Small Business Eligibility Decision	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).	Met
SH-111	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Provide the capability to capture information and details of a Employer complaint.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-112	Small Business	Appeal Small Business Eligibility Decision	OneGate	Allow employers to review record of participation in the Small Business Exchange.	Met
SH-114	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Provide the capability for an employer to request an appeal to the employer eligibility decision.	Validated
SH-115	Small Business	Appeal Small Business Eligibility Decision	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.	Duplicate
SH-116	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Provide the capability to capture, track, and disposition appeals in the Exchange (including status, assignments, and relevant case notes).	Validated
SH-117	Small Business	Appeal Small Business Eligibility Decision	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.	Validated
SH-118	Small Business	Appeal Small Business Eligibility Decision	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).	Met
SH-119	Small Business	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Provide the capability to record the detailed results and supporting documentation that result from or support an appeals decision.	Validated
SH-120	Small Business	Appeal Small Business Eligibility Decision	OneGate	Generate a formal written notice informing an employer of the details of an appeal decision.	Duplicate
SH-123	Small Business	Renew / Redetermine Employer Participation	OneGate	Provide capability for employers to submit changes to employee roster (add / remove employees) in between redeterminations / renewals.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-124	Small Business	Change Reporting	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.)	Validated
SH-125	Small Business	Renew / Redetermine Employer Participation	OneGate	Upon reporting changes in offers of coverage to all Full Time Employees, Employers must self-attest to continue participation in Small Business.	Validated
SH-127	Small Business	Change Reporting/Periodic Reporting	OneGate	Provide capability for employers to check the status of employee QHP enrollment through the web portal.	Validated
SH-129	Small Business	Change Reporting/Periodic Reporting	OneGate	Provide the capability to recalculate the employer's total cost based on reported changes to the employee roster.	Validated
SH-130	Small Business	Update Employee Application	OneGate	Provide the capability for employers to submit changes to the employer contact information.	Validated
SH-132	Small Business	Update Employee Application	OneGate	Prepare and send communication to the employer regarding changes to the Employer contact information.	Validated
SH-133	Small Business	Renew / Redetermine Employer Participation	OneGate	Initiate the termination process if the employer is to be found no longer eligible for the Exchange.	Validated
SH-134	Small Business	Renew / Redetermine Employer Participation	OneGate	Provide the capability for employers to submit changes about the employer's principal business address or primary worksite location.	Validated
SH-135	Small Business	Renew / Redetermine Employer Participation	OneGate	Provide the ability to capture a reported change in the employer's principal business location and satellite offices.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-138	Small Business	Renew / Redetermine Employer Participation	OneGate	Provide the capability to determine employer eligibility based on the employer's principal business location and satellite offices.	Validated
SH-139	Small Business	Renew / Redetermine Employer Participation	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.	Validated
SH-141	Small Business	Renew/Redetermine Employer Participation	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.	Validated
SH-142	Small Business	Prepare Employee Application	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 election status on behalf of their employees (i.e. log or complete the waiver process) while requiring employee approval/recognition.	Validated
SH-143	Small Business	Prepare Employee Application	OneGate	To confirm Small Business eligibility, first request that employee log-in with user name and password.	Met
SH-144	Small Business	Prepare Employee Application	Oracle Identity Manager	Prompt employees to update all account information, including the password upon initial log in.	Deleted
SH-145	Small Business	Verify Employee Application Data	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.	Validated
SH-146	Small Business	Verify Employee Application Data	OneGate	Provide capability to verify if employee exists on employee roster in order to verify an employee's coverage through an employer.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-147	Small Business	Verify Employee Application Data	OneGate	Display the result of the verification process.	Met
SH-148	Small Business	Determine Employee Eligibility	OneGate	Update user /employee account status based on updated employee coverage results	Met
SH-149	Small Business	Determine Employee Eligibility	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.	Met
SH-151	Small Business	Prepare Employee Application	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 - Employer Name - Worksite Address	Validated
SH-152	Small Business	Prepare Employee Application	OneGate	Provide the capability to use the model single employee application provided by HHS.	Validated
SH-153	Small Business	Prepare Employee Application	OneGate	Provide additional language support in accordance with Exchange language support guidelines.	Validated
SH-154	Small Business	Prepare Employee Application	OneGate	Provide field level help for each application data element that includes description and required data format.	Met
SH-155	Small Business	Prepare Employee Application	OneGate	Provide capability for employees to access in-depth online help during the application process.	Validated
SH-157	Small Business	Prepare Employee Application	OneGate	During the Application Process, prompt the Employee to enter the exact name associated with the SSN.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-158	Small Business	Prepare Employee Application	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.	Validated
SH-159	Small Business	Prepare Employee Application	OneGate	Provide the capability to identify Navigators (or Brokers, etc.) if they are completing applications on behalf of an employee.	Validated
SH-160	Small Business	Prepare Employee Application	OneGate	Accept paper documents for Small Business, including employee applications.	Validated
SH-161	Small Business	Prepare Employee Application	OneGate	Validate field-level information for correct data format and completeness.	Met
SH-162	Small Business	Prepare Employee Application	Loqate	Conduct validation of mailing addresses provided in applications through attestation	Validated
SH-163	Small Business	Prepare Employee Application	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.	Validated
SH-164	Small Business	Prepare Employee Application	OneGate	For employees who do not have a SSN, allow the application process to proceed.	Validated
SH-165	Small Business	Prepare Employee Application	OneGate	Within the QHP application, the Exchange shall validate field-level information for format and completeness.	Met
SH-166	Small Business	Prepare Employee Application	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	Met
SH-167	Small Business	Prepare Employee Application	OneGate	Save application information to user account after account creation.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-168	Small Business	Prepare Employee Application	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)	Met
SH-169	Small Business	Prepare Employee Application	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.	Validated
SH-170	Small Business	Prepare Employee Application	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	Validated
SH-171	Small Business	Employee Selects QHP	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.	Deleted
SH-172	Small Business	Employee Selects QHP	OneGate	Produce a real-time electronic request to the employee to determine employee preferences for qualified health plan(s).	Deleted
SH-173	Small Business	Employee Selects QHP	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 - Date of Birth - Address - Phone Number - Gender - Smoking Status - Indian Status	Validated
SH-174	Small Business	Verify Indian Status	OneGate	Provide capability to validate employee Indian status of employee and/or dependent(s) submitted through the employee application.	Deleted
SH-175	Small Business	Plan Selection	OneGate	Based on carrier and plan information gathered, display plan cost and availability.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-176	Small Business	Employee Selects QHP	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.	Met
SH-177	Small Business	Employee Selects QHP	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.	Met
SH-178	Small Business	Employee Selects QHP	OneGate	Provide capability to display a detailed comparison of available employer-selected health plans based on employee preferences	Validated
SH-179	Small Business	Employee Selects QHP	OneGate	Store enrollment questionnaire responses and display plan choices based on application / filtering criteria.	Deleted
SH-180	Small Business	Employee Selects QHP	OneGate	Provide capability to view and select plan(s) for employee dependents, if covered by employer	Validated
SH-181	Small Business	Employee Selects QHP	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.	Deleted
SH-182	Small Business	Employee Selects QHP	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 choices, and the ability to view all available plans based on a specified tier based on employer selection.	Met
SH-183	Small Business	Employee Selects QHP	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 mandate, due to federal law. If either is scenario is likely, invite employee to explore these options further at the Individual Exchange.	Validated
SH-184	Small Business	Employee Selects QHP	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	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-185	Small Business	Employee Selects QHP	OneGate	Provide capability for an employee to select QHP(s) and initiate the enrollment process.	Validated
SH-186	Small Business	Employee Selects QHP	OneGate	Update an employee's account to reflect plan selection and the effective projected plan-year.	Validated
SH-187	Small Business	Employee Selects QHP	3rd Party Premium Processor	After plan selection, initiate the financial transactions required by employers to ensure plan enrollment process / transaction to applicable carriers.	Validated
SH-188	Small Business	Employee Selects QHP	OneGate	After acknowledgement of the receipt of the plan selection, initiate the calculation of the final cost to employee	Validated
SH-189	Small Business	Employee Selects QHP	OneGate	After acknowledgement of the receipt of the plan selection, display the calculation of the final cost (net premium) to employee	Met
SH-190	Small Business	Employee Selects QHP	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.	Validated
SH-192	Small Business	Employee Selects QHP	OneGate	Provide the capability to verify and acknowledge the receipt of the plan selection.	Met
SH-193	Small Business	Employee Selects QHP	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	Validated
SH-195	Small Business	Employee Enrollment in QHP	OneGate	Receive and process acknowledgement of employee enrollment from Issuer	Validated
SH-198	Small Business	Update Employee Eligibility Application	OneGate	Allow employees to enroll in QHP during a qualifying event.	Validated
SH-199	Small Business	Disenroll Employee in QHP	OneGate	Provide the capability for an employee to request a voluntary disenrollment from QHP(s).	Validated
SH-201	Small Business	Disenroll Employee in QHP	OneGate	If an employee initiates a voluntary disenrollment through the Exchange, produce an electronic notification to the Issuer to disenroll the employee.	Validated
SH-202	Small Business	Disenroll Employee in QHP	OneGate	Provide capability to initiate the disenrollment process.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-203	Small Business	Disenroll Employee in QHP	OneGate	Provide capability to update user accounts based on disenrollment notification from issuers	Validated
SH-204	Small Business	Disenroll Employee in QHP	OneGate	Update user accounts based on disenrollment notification from disenrollment initiated by the Exchange.	Validated
SH-206	Small Business	Disenroll Employee in QHP	??	Provide capability to receive electronic notifications from Issuers regarding disenrollment and initiate disenrollment process.	Validated
SH-209	Small Business	Disenroll Employee in QHP	OneGate	If conditions for an involuntary disenrollment are met, initiate the disenrollment process.	Validated
SH-211	Small Business	Disenroll Employee in QHP	OneGate	Update user accounts based on disenrollment notification from issuers or disenrollment initiated by the Exchange.	Validated
SH-214	Small Business	Update Employee Application / Renew Employee QHP Participation	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 identity is confirmed.	Validated
SH-215	Small Business	Renew Employee QHP Participation	OneGate	Track annual renewal date for employers.	Validated
SH-216	Small Business	Update Employee Application / Renew Employee QHP Participation	OneGate	Based on employee status, determine eligibility for Small Business Exchange participation renewal.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-218	Small Business	Update Employee Application / Renew Employee QHP Participation	Oracle Identity Manager	Provide capability for employees to look up or reset login credentials.	Validated
SH-221	Small Business	Update Employee Application	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.	Deferred
SH-222	Small Business	Update Employee Application	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 eligibility and enrollment.	Deferred
SH-223	Small Business	Renew Employee QHP Participation	OneGate	Provide the capability to calculate a year-to-date average for premiums paid for display to the employee at time of renewal.	Deferred
SH-224	Small Business	Update Employee Application	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.	Deferred
SH-225	Small Business	Renew Employee QHP Participation	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.	Deleted
SH-226	Small Business	Renew Employee QHP Participation	OneGate	Based on the availability of QHP(s), determine availability of an employee's current plan for the purposes of enrollment renewal.	Deleted
SH-227	Small Business	Update Employee Application	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 through the Exchange.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-228	Small Business	Renew Employee QHP Participation	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.	Deleted
SH-229	Small Business	Employee Enrollment in QHP	OneGate	Process notification to employer of coverage for employees. Also, communicate any next steps required by the employer.	Validated
SH-230	Small Business	Determine Employee Eligibility	OneGate	Provide the functionality to determine if an update to an employee account is categorized as a Qualifying Event.	Validated
SH-231	Small Business	Update Employee Application	OneGate	Provide capability for employees to submit changes to employee plan (add / remove dependents) in between redeterminations / renewals and due to qualifying events.	Validated
SH-234	Small Business	Change Reporting	OneGate	Initiate enrollment or disenrollment process for employee or the employee's dependents, depending on the nature of the Qualifying Event.	Validated
SH-235	Small Business	Change Reporting	OneGate	Provide the capability for employees to submit changes to the employee contact information.	Validated
SH-238	Small Business	Periodic Reporting and Reconciliation	OneGate	Allow employers and brokers/assisters to view and track the premium payment.	Validated
FM-001	Financial Management	Fed APTCs and CSRs	CGI	Generate daily transactional 834 transaction file in a HIPAA compliant format on all individuals enrollment updates for the Exchange	Validated
FM-002	Financial Management	Fed APTCs and CSRs	CGI	Transmit daily transactional 834 transaction file in a HIPAA compliant format of individuals enrolled in QHPs to CMS	Validated
FM-003	Financial Management	Fed APTCs and CSRs	CGI	Generate monthly 834 transaction file in a HIPPA compliant format of individuals enrolled in QHPs, including Federal APTC, CSR amounts to support the monthly reconciliation process with CMS and Issuers.	Validated
FM-004	Financial Management	Fed APTCs and CSRs	CGI	Transmit monthly 834 transaction file in a HIPPA compliant format of individuals enrolled in QHPs, including Federal APTC, CSR and State Premium Subsidy and CSR amounts to CMS to support the monthly reconciliation process with CMS.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
FM-005	Financial Management	Fed APTCs and CSRs	CGI	Transmit monthly 834 transaction file in a HIPPA compliant format of individuals enrolled in QHPs, including Federal APTC, CSR and State Premium Subsidy and CSR amounts to Issuers to support the monthly reconciliation process with Issuers.	Validated
FM-006	Financial Management	Fed APTCs and CSRs	CGI	Update Exchange financial data with Federal APTC, CSR and State Premium Subsidy, CSR payments to Issuers for updating into the State's General Ledger, and forward to the Premium Processor.	Validated
FM-009	Financial Management	Fed APTCs and CSRs	CGI	Receive electronic reports of payments from CMS to Issuers for federal APTC and CSR amounts	Validated
FM-011	Financial Management	APTCs and CSRs	CGI	Provide the ability to identify, analyze and resolve Federal APTC and Federal CSR discrepancies between CMS and the Exchange Eligibility and Enrollment data store	Validated
FM-012	Financial Management	Fed APTCs and CSRs	CGI	Update State's G/L (Vision) system with electronic Issuer Federal APTC/CSR payment data	Validated
FM-014	Financial Management	Fed APTCs and CSRs	CGI	Provide tool to adjust identified discrepancies between the Vision database and data received from Issuers, and/or CMS	Deleted
FM-018	Financial Management	Fed APTCs and CSRs	CGI	Update Individual Eligibility and Enrollment database to reflect discrepancy resolution between CMS, Issuer, HBE and Premium Processor	Validated
FM-027	Financial Management	Small Business Premium Collection	CGI	Provide functionality that allows a Small Business to create a notification that invoice discrepancy exists.	Validated
FM-033	Financial Management	Small Business Premium Collection	CGI	Provide the ability for small businesses to view payment history and data.	Validated
FM-034	Financial Management	Small Business Premium Collection	CGI	Identify and account for discrepancies between Small Business payments and CMS reported payments (reconciliation).	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
FM-044	Financial Management	State Option to Collect Individual Premiums through the Exchange	CGI	Provide the ability for an individual to view their invoice online.	Validated
FM-045	Financial Management	State Option to Collect Individual Premiums through the Exchange	CGI	Provide invoice discrepancy notification capabilities for Individual to Exchange.	Validated
FM-053	Financial Management	State Option to Collect Individual Premiums through the Exchange	CGI	Provide the ability for individual users to view payment history and data.	Validated
FM-059	Financial Management	Small Business Premium Discrepancy Resolution	CGI	Receive Small Business invoice discrepancy notification.	Validated
FM-060	Financial Management	Small Business Premium Discrepancy Resolution	CGI	Provide inquiry screens to research the Small Business discrepancy	Validated
FM-061	Financial Management	Small Business Premium Discrepancy Resolution	CGI	Notify authorized users of the Small Business reported discrepancy.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
FM-062	Financial Management	Small Business Premium Discrepancy Resolution	CGI	Provide capability for small businesses to update small business account and make adjustments.	Validated
FM-070	Financial Management	Individual Premium Discrepancy Resolution	CGI	Provide ability for Individuals to log into Exchange and view notifications and invoice	Duplicate
FM-072	Financial Management	Individual Premium Discrepancy Resolution	CGI	Provide automated process to identify invoice discrepancies from an individual.	Deleted
FM-073	Financial Management	Individual Premium Discrepancy Resolution	CGI	Provide notification to individual that discrepancy report was received from the individual.	Deleted
FM-074	Financial Management	Individual Premium Discrepancy Resolution	CGI	Provide inquiry screens to research the individual and family units discrepancy	Validated
FM-075	Financial Management	Individual Premium Discrepancy Resolution	CGI	Notify authorized users of the reported Individual or Family Unit discrepancy.	Validated
FM-082	Financial Management	Issuer Payment Reconciliation	CGI	Receive electronic or telephonic notification of discrepancy from Issuer.	Validated
FM-085	Financial Management	Issuer Payment Reconciliation	CGI	The system will provide screens to update Exchange records with corrected invoice / payment information for Issuers, Small Businesses, or Individual (including Family Unit) records.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
FM-086	Financial Management	Risk Adjustment Calculation	CGI	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 effective dates for individual and small group market non-grandfathered plans.	Deleted
FM-087	Financial Management	Risk Adjustment Calculation	CGI	Provide regular reports and data on QHPs and encounters to CMS to support risk adjustment calculation.	Deleted
FM-088	Financial Management	Risk Adjustment Calculation	CGI	Provide the capacity to electronically receive information from Issuers on non-exchange enrollees from individual, Small Business and self-funded plans inside and outside of the state	Deleted
FM-089	Financial Management	Risk Adjustment Calculation	CGI	Provide the capacity to electronically receive non QHP plan and rate setting data from CMS and other state sources	Deleted
FM-090	Financial Management	Risk Corridors	CGI	Extract and send Individual and SHOP Plan data to CMS for risk corridors	Deleted
FM-091	Financial Management	Risk Corridors	CGI	Receive unpaid Risk Corridor Charge information from CMS	Deleted
FM-106	Financial Management	Exchange Internal Accounting	CGI	Track operational and overhead expenses of the Exchange.	Deleted
FM-107	Financial Management	Exchange Internal Accounting	CGI	The Exchange system will summarize and apply general ledger coding to the financial transactions	Validated
FM-108	Financial Management	Exchange Internal Accounting	CGI	The Exchange system will update Vision with aggregated financial information	Validated
FM-109	Financial Management	Exchange Internal Accounting	CGI	Transmit the general ledger transactions to the accounting system.	Duplicate
FM-110	Financial Management	Exchange Internal Accounting	CGI	The Exchange will provide detail reports to support and reconcile the Exchange Annual Financial Report	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
FM-111	Financial Management	Exchange Internal Accounting	CGI	The Premium Processor shall provide annual SSAE No. 16 report to the State	Validated
FM-112	Financial Management	Exchange Internal Accounting	CGI	The System shall create regular and ad-hoc reporting on an as-needed basis to govern and monitor the Exchange financial health based on the HBE data store	Validated
FM-113	Financial Management	Exchange Internal Accounting	CGI	Provide selected financial information required to support building the Exchange Annual Financial Report as required by CMS and other state entities, including information sent by Premium Processor to the HBE data store	Validated
New-002	Financial Management	State premium subsidies	CGI	Quarterly, report to the State the state premium subsidy payments that have not been forwarded to the Issuer due to a lack of matching premium payments from the individual.	Validated
New-004	Financial Management	Exchange Internal Accounting	CGI	The Exchange System will provide the tools and information required to support the audit of the financial aggregate report from the General Ledger through to the Premium Processor financial transactions.	Validated
New-005	Financial Management		CGI	The Exchange system shall provide an aggregated report in a GAAP compliant format for each Individual and Family Unit: • QHP premiums due for a reporting period (month) • Payments made, period to date (month) • Payments applied to QHP premiums for a period (month)	Validated
New-006	Financial Management		CGI	The Exchange system provide an aggregated report in a GAAP compliant format for each Small Business: • QHP Premiums for a reporting period (month) • Payments made, period to date (month) • Payments applied to QHP premiums for a period (month)	Validated
New-007	Financial Management		CGI	The Exchange system shall provide an aggregated report in a GAAP compliant format for each Individual and Family Unit: • Federal APTC/CSR subsidy calculated for an Individual for a reporting period (month) • Federal APTC/CSR subsidy payment paid to the Issuer for an Individual for a reporting period (month)	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
New-008	Financial Management		CGI	The Exchange system shall provide an aggregated report in a GAAP compliant format for each Individual and Family Unit: • State Premium Subsidy and State CSR calculated for an Individual for a reporting period (month) • State premium subsidy and State CSR paid to the Issuer for an Individual for a reporting period (month)	Validated
New-009	Financial Management		CGI	The Exchange system shall provide the State transaction financial information weekly.	Validated
New-012	Financial Management		CGI	The Exchange system shall provide an aggregated report where the information is GAAP compliant with details available for Individual NSF transaction summaries.	Deferred
New-013	Financial Management		CGI	The Exchange system shall provide real-time access to financial data to support Exchange operations including real-time customer service and self service.	Validated
New-016	Financial Management		CGI	The System shall provide Premium Processing costs to the State monthly.	Validated
New-017a	Financial Management		CGI	The System shall provide monthly reports on credit card fees.	Validated
New-018	Financial Management	State Premium Subsidy and CSR	CGI	The System shall generate a file of individuals enrolled in QHPs, including State Premium Subsidy, State CSR amounts to support the monthly reconciliation process with State and Issuers	Validated
New-019	Financial Management	Eligibility and State Premium Subsidy and CSR	CGI	Establish individual eligibility and determine State Premium Subsidy amount.	Validated
New-020	Financial Management	Eligibility and State Premium Subsidy and CSR	CGI	Establish individual eligibility and determine State CSR amount.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
New-021	Financial Management	Federal APTC and CSR, State Premium Subsidy and CSR	CGI	Transmit daily transactional 834 transaction file in a HIPAA compliant format of individuals enrolled in QHPs to CMS generate Individual enrollment updates from the Exchange, including Federal APTC and CSR and State Premium Subsidy and State CSR amounts to the Premium Processor.	Validated
New-022	Financial Management	Eligibility and APTC and CSR	CGI	Transmit daily Individual enrollment updates from the Exchange, including eligibility and Federal APTC and Federal CSR, State Premium Subsidy and Federal CSR amounts to the Premium Processor.	Validated
New-023	Financial Management	State Premium Subsidy and CSR	CGI	Generate daily transactional file on all individual enrollment updates for the Exchange including State CSR amounts	Validated
New-024	Financial Management	State Premium Subsidy and CSR	CGI	Transmit daily transactional file on all individuals enrolled in QHPs including State CSR amounts to Issuers	Validated
New-100		Individual Premium Discrepancy Resolution	CGI	Send premium payment reports via EDI 820 transactions to the Issuers.	Validated
New-101		Small Business	CGI	Send premium payment reports via EDI 820 transactions to the Issuers.	Validated
New-101		Small Business	CGI	Send premium payment reports to the State's Medicaid Business Office.	Validated
New-103	Financial Management	Exchange/State Agencies	CGI	Send termination notification to the Premium Processor.	Validated
New-106		Individual Premium Discrepancy Resolution	CGI	Receive notification of termination from Issuers	Validated
New-107		Individual Premium Discrepancy Resolution	CGI	Send notification of termination to Premium Processor	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
New-108		Small Business	CGI	Receive notification of termination from Issuers	Validated
New-109		Small Business	CGI	Send notification of termination to Premium Processor	Validated
New-120		State Premium Subsidy and CSR	CGI	Receive actual State CSR due amounts from the Issuers, and forward to Premium Processor.	Validated
New-130		Fed APTCs and CSRs	CGI	Receive electronic payment history report from Issuers and forward to the Premium Processor	Validated
PPRFP-002	Financial Management	State Option to Collect Individual Premiums through the Exchange	CGI	Provide an electronic method for use by each family unit, navigator/broker/in-person assistor or customer service agent to set up a premium payment account.	Validated
PPRFP-003	Financial Management	State Option to Collect Individual Premiums through the Exchange	CGI	Enable each family unit to choose the manner by which it will receive notifications (e.g., invoices, correspondence).	Validated
PPRFP-023	Financial Management	State Option to Collect Individual Premiums through the Exchange	CGI	Receive termination notification from the Issuer and the State's Medicaid Business Office.	Validated
PPRFP-033	Financial Management	Small Business	CGI	Provide an electronic method for use by each small business, navigator/broker/in-person assistor or customer service agent to set up a premium payment account.	Validated
PPRFP-034	Financial Management	Small Business	CGI	Enable each small business to choose the manner (e.g., electronic, paper) by which it will receive notifications (e.g., invoices, correspondence).	Validated
CACM-01	Consumer Assistance	Case Management	OneGate	Provide the ability to add multiple dated narratives to a case and track and maintain changes over time via the narratives.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
CACM-02	Consumer Assistance	Case Management	OneGate	Maintain a history of notices that have been sent to a individual, employer, Navigator, Broker.	Met
CACM-03	Consumer Assistance	Case Management	OneGate	Maintain and a history of a individual's eligibility status over time.	Met
CACM-04	Consumer Assistance	Case Management	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.	Met
CACM-05	Consumer Assistance	Case Management	OneGate	Allow Caseworkers and Customer Support staff to deactivate a particular customer's case.	Met
CACM-06	Consumer Assistance	Case Management	OneGate	Allow Caseworkers and Customer Support staff shall to reactivate a client's case based on new information, new application or redetermination.	Met
CACM-07	Consumer Assistance	Case Management	OneGate	Provide mechanism to check and flag duplicate individual cases.	Met
CACM-08	Consumer Assistance	Case Management	OneGate	Allow Customer Service Supervisors to merge multiple individual cases into one, or split single cases into multiples cases when they deem it warranted.	Validated
CACM-09	Consumer Assistance	Case Management	OneGate	Allow Caseworkers and Customer Support staff to mark a case duplicate, but remain unmerged.	Met
CACM-10	Consumer Assistance	Case Management	OneGate	Allow Caseworkers and customer support staff the ability to search for a specific individuals' information.	Met
CACM-11	Consumer Assistance	Case Management	OneGate	Allow Caseworkers and Customer Support staff to view individual information entered into the Portal from the Case Mgmt system.	Met
CACM-12	Consumer Assistance	Case Management	OneGate	Allow Caseworkers and Customer Support Staff to add to a individual's information.	Met
CACM-13	Consumer Assistance	Case Management	OneGate	Allow Caseworkers and Customer Support Staff to change or modify an individual's information.	Met
CACM-14	Consumer Assistance	Customer Application Intake Process	OneGate	Allow Caseworkers and Customer Support staff to search for the individual's eligibility details.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
CACM-15	Consumer Assistance	Customer Application Intake Process	OneGate	Allow Caseworkers and Customer Support Staff to view the individual's eligibility details (e.g., income sources, citizenship, immigration status, etc.).	Met
CACM-16	Consumer Assistance	Customer Application Intake Process	OneGate	Allow Caseworkers and Customer Support staff to add new data into the individual's eligibility details (income sources, citizenship, immigration status, etc.).	Met
CACM-17	Consumer Assistance	Case Management--Administration	OneGate	Provide a mechanism for role-based access control for any changes to the rules or parameters in the rules engine.	Met
CACM-18	Consumer Assistance	Case Management--Administration	OneGate	Track changes made to an account in an auditable log.	Met
CACM-20	Consumer Assistance	Case Management--System Access	OneGate	Allow supervisors to enter the system through a customized portal to view and manage all the cases of the caseworkers under their jurisdiction.	Met
CACM-21	Consumer Assistance	Case Management--System Access	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.	Met
CAG-01	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system must support the complaints/appeals process.	Met
CAG-02	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall allow customer support representative to log customer complaints and appeals.	Duplicate
CAG-03	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall allow staff to attach relevant documents to complaint or appeal.	Met
CAG-04	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	Associated recorded calls/transcripts and online chat sessions log with the appropriate appeal	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
CAG-05	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall prompt customer support representative on complaints/grievances/ appeals/fair hearings workflow by integrating with workflow/document management system.	Validated
CAG-06	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system will track time frames and deadlines for responding to complaints and appeals.	Met
CAG-07	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall allow customer support representative to generate letters to consumer throughout grievance/appeals/fair hearings/complaints process.	Met
CAG-08	Consumer Assistance	Complaints / Appeals	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.	Met
CAG-09	Consumer Assistance	Complaints / Appeals	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.	Met
CAG-10	Consumer Assistance	Complaints / Appeals	OneGate	The rules engine must reflect changes in enrollment, coverage, and tax credits as a result of a complaint, grievance, and appeal decision.	Met
CAG-11	Consumer Assistance	Complaints / Appeals	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.	Validated
CAG-12	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall allow consumers to submit complaint/appeal via phone, web, chat session, email, and letter.	Validated
CAG-13	Consumer Assistance	Complaints / Appeals	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.	Validated
CAG-14	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall monitor appeals/complaints due dates and alert staff or management of overdue status.	Validated
CAG-15	Consumer Assistance	Complaints / Appeals	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.	Validated
CAG-16	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall have the ability to assign a priority, or level to the appeal/complaint.	Met
CAG-19	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall support outreach initiatives using letters, emails, phone calls, text messages as described below.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
CAG-20	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	The system shall ask and store consumers' preferred method of communication.	Met
CAG-23	Consumer Assistance	Outreach / Education	OneGate	The system shall support multi-lingual communication in at least the languages specified by the Exchange, and may able to support additional language (including languages that use non-Western scripts).	Met
CAG-24	Consumer Assistance	Outreach / Education	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.	Met
CAG-29	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	The system shall flag consumer assistance staff or Navigators whenever a consumer calls and queries pre-defined questions.	Validated
CAG-31	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	The system shall capture information on outreach efforts (e.g. how did you hear about us?).	Met
CAG-32	Consumer Assistance	Workflow	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	Validated
CAG-33	Consumer Assistance	Workflow	Siebel Public Sector CRM	The system shall have the ability to integrate voice and electronic transactions into a single workflow.	Deferred
CAG-34	Consumer Assistance	Workflow	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.	Validated
CAG-35	Consumer Assistance	EDM	ThunderHeadNOW	Support electronic document management (EDM) capabilities	Met
CAG-36	Consumer Assistance	EDM	ThunderHeadNOW	The system shall provide the ability to upload attachments to all individual and correspondence records.	Met
CAG-37	Consumer Assistance	EDM	Siebel Public Sector CRM	The system shall provide the ability to view related correspondence records from a single correspondence record.	Validated
CAG-39	Consumer Assistance	EDM	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).	Met
CAG-40	Consumer Assistance	Contact Tracking	Siebel Public Sector CRM	The system shall assign a unique number to identify each instance of a contact.	Met
CAG-41	Consumer Assistance	Contact Tracking	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.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
CAG-42a	Consumer Assistance	Contact Tracking	Siebel Public Sector CRM	The system shall track and search on contacts with basic identifying information such as time and date of contact, caller name, contact type, reason or any combination thereof.	Validated
CAG-42b	Consumer Assistance	Contact Tracking	Siebel Public Sector CRM	The system shall track and search on contacts with basic identifying information such as Provider number, member number, agent ID, status of issue, or any combination thereof.	Validated
CAN-01	Consumer Assistance	Navigators	OneGate	Provide consumers with general information regarding Navigator Program, including information regarding certification of Navigators and relationship to Exchange, Issuers, Providers and Brokers	Met
CAN-02	Consumer Assistance	Navigators	OneGate	Allow certified Navigators to enter the portal through a distinct login.	Validated
CAN-03	Consumer Assistance	Navigators	OneGate	Allow Navigators to create an account with the Exchange.	Validated
CAN-04	Consumer Assistance	Navigators	OneGate	Require Navigators to provide credentials and certification information to establish an account.	Validated
CAN-05a	Consumer Assistance	Navigators	OneGate	Allow consumers to see the Navigator's credentials and certification information and select a Navigator based on them.	Validated
CAN-05b	Consumer Assistance	Navigators	OneGate	Flag Management if Navigator information is not up to date, or on probation for misconduct.	Deferred
CAN-06	Consumer Assistance	Navigators	OneGate	Verify the information provided by the Navigator.	Deferred
CAN-07	Consumer Assistance	Navigators	OneGate	Create an account for the Navigator and assign a unique ID that will be maintained in the Navigator account.	Validated
CAN-08	Consumer Assistance	Navigators	OneGate	Track the number of persons assisted by each Navigator on a monthly basis and produce detailed reports on such activity.	Duplicate
CAN-09	Consumer Assistance	Navigators	OneGate	Generate reports by Navigator; determining effectiveness by community, population, enrollment.	Duplicate
CAN-11	Consumer Assistance	Navigators	OneGate	Provide a process to provide feedback or communication to the Navigators, in order for state agencies to communicate information	Validated
CAN-12	Consumer Assistance	Navigators	OneGate	The system shall flag Management if Navigator has performance issues (e.g.., missing deadlines, aging and outstanding customer inquiries, incomplete applications, enrollment, etc.).	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-042	Consumer Assistance	Evaluate QHP Issuer Application	TBD	Provide ability for Issuers to provide relevant Complaint and Compliance Information	Validated
PM-120	Consumer Assistance	Maintain Operational Data	TBD	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 include: - Issuer - Plan - Number of complaints - Complaint type - Complaint description/detail	Validated
PM-121	Consumer Assistance	Maintain Operational Data	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	Met
PM-122	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Provide automatic electronic notification of receipt for complaints submitted through the web interface.	Met
PM-123	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Allow Exchange users such as consumers, navigators, etc. to log into their Exchange account to post/submit a complaint	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-124	Consumer Assistance	Maintain Operational Data	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 - Plan Involved - Number and Type of Complaint - Complaint rates - Complaint response time	Validated
PM-125	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Track and manage complaints for the Exchange	Met
PM-126	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Use a common, standard format for complaint data from all sources to facilitate merging complaint data for analysis.	Validated
PM-127	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Allow complaint managers to classify complaints by attributes to support triaging complaints for action or referral	Met
PM-128	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Retain the source of the complaint (i.e. provider, issuer, Insurance Division, etc.) and the date received	Validated
PM-129	Consumer Assistance	Maintain Operational Data	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	Validated
PM-130	Consumer Assistance	Maintain Operational Data	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, communication tracking, contacts, etc.	Validated
PM-131	Consumer Assistance	Maintain Operational Data	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	Validated
PM-132	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Notify a complaint worker that a complaint has been assigned/routed to that person	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-133	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Allow reassignment of a complaint to a new complaint worker	Met
PM-136	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Publish approved complaint data summaries on the Exchange web portal for customer review , and to support transparency.	Validated
PM-137	Consumer Assistance	Maintain Operational Data	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 - Complaint type - Complaint description/detail	Validated
PM-138	Consumer Assistance	Maintain Operational Data	Siebel Public Sector CRM	Provide the capability to send an electronic complaint referral to: - An Issuer - OIC - Eligibility case/complaint workers - Exchange customer service - Others (to be defined)	Validated
SH-111	Consumer Assistance	Appeal Small Business Eligibility Decision	Siebel Public Sector CRM	Provide the capability to capture information and details of a Employer complaint.	Validated
SH-121	Consumer Assistance	Appeal Small Business Eligibility Decision	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.	Validated
SH-156	Consumer Assistance	Prepare Employee Application	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.	Deferred
MO-1	Consumer Assistance	CRM/Call Center Functionality	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.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
MO-2	Consumer Assistance	CRM/Call Center Functionality	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.	Validated
MO-3	Consumer Assistance	CRM/Call Center Functionality	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).	Met
MO-4	Consumer Assistance	CRM/Call Center Functionality	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.	Validated
MO-5	Consumer Assistance	CRM/Call Center Functionality	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.	Met
MO-6	Consumer Assistance	CRM/Call Center Functionality	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).	Validated
MO-7	Consumer Assistance	CRM/Call Center Functionality	Siebel Public Sector CRM	The CRM solution shall seamlessly 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	Validated
MO-8	Consumer Assistance	CRM/Call Center Functionality	Siebel Public Sector CRM	The system shall maintain a record of inquiry and correspondence data online, with periodic backups managed by CGI. The call center shall be able to store record of recordings of assisted calls, in a time frame specified by the Exchange.	Validated
MO-9	Consumer Assistance	CRM/Call Center Functionality	Siebel Public Sector CRM	The system shall provide functionality that is capable of integrating with the integration tool to support billing, Enrollment/Eligibility, the secured access to the Case Management, and data integration with call management system.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
MO-10	Consumer Assistance	CRM/Call Center Functionality	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.	Validated
MO-11	Consumer Assistance	CRM/Call Center Functionality	Siebel Public Sector CRM	The system shall have the ability to enable security around confidential consumer data allowing designated staff access.	Validated
MO-12	Consumer Assistance	IVR Technology	Siebel Public Sector CRM	The system shall interface with and support the use of an IVR system.	Validated
MO-13	Consumer Assistance	ACD Technology	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.	Deferred
MO-14	Consumer Assistance	ACD Technology	Siebel Public Sector CRM	The system shall provide capability to prioritize agents by availability, skill set, language, and overflow from other queues.	Deferred
MO-15	Consumer Assistance	ACD Technology	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.	Deferred
MO-16	Consumer Assistance	ACD Technology	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.	Deferred
MO-17	Consumer Assistance	ACD Technology	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).	Deferred
MO-18	Consumer Assistance	ACD Technology	Siebel Public Sector CRM	The system will alert management and staff when service levels are not being met.	Deferred
MO-19	Consumer Assistance	ACD Technology	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.	Deferred

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
MO-20	Consumer Assistance	ACD Technology	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	Deferred
MO-21	Consumer Assistance	ACD Technology	Siebel Public Sector CRM	The system shall allow authorized managers or supervisors to monitor active calls.	Deferred
MO-22	Consumer Assistance	ACD Technology	Siebel Public Sector CRM	The system shall provide the capability to record all call interactions	Deferred
CAG-46	Consumer Assistance	Quality Monitoring	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	Deferred
A-1	Audit	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)	Validated
A-2	Audit	Eligibility Determination	OneGate	Maintain data to produce a report of the outcomes of rules execution for all eligibility determinations (positive or negative) for appeals research and to analyze correctness of eligibility functionality.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
A-3	Audit	Transfer of Identification Information	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).	Validated
A-4	Audit	IRS Tax Information	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.	Validated
A-5	Audit	Risk Adjustment, Risk Corridors, and Reinsurance	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.	Validated
A-6	Audit	Security	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.	Validated
A-8	Program Integrity	Identity Management	Oracle Enterprise Data Quality	Retain sufficient data to allow periodic sampling and analysis to identify potential fraud, waste, and abuse.	Validated
A-10	Program Integrity	Individual Identification	Oracle MDM (Customer Hub)	Retain sufficient data to allow periodic analysis of potentially duplicate individuals	Validated
A-12	Program Integrity	Individual Identification	Oracle MDM (Customer Hub)	Provide the ability to successfully merge/unmerge potential duplicate individual records	Validated
A-9	Program Integrity	Individual Identification	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
	Web Analytics	Web Analytics	Google Analytics	Provide web analytics tools comparable to Google Analytics	Validated
	Web Analytics	Web Analytics	Splunk	Provide the capability to review raw web logs for usability and security analyses	Deferred
A-19	Business Analytics	SHOP, EE,Plan Management	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 - Individual and employee financial data - Premium and CSR subsidy data - Enrollment data - Enrollee demographics	Validated
A-20	Business Analytics	Platform	Oracle BI	The business analytics solution for the Exchange should not impact transactional database performance.	Validated
A-21	Business Analytics	Platform	Oracle BI	The system must provide the ability to generate ad hoc reports.	Validated
A-22	Business Analytics	Platform	Oracle BI	The system must provide the ability to download and save report data to individual workstations and applications.	Validated
A-23	Business Analytics	Platform	Oracle BI	The system must provide the ability to transmit reports to various designated recipients in a secure manner.	Validated
A-24	Business Analytics	Platform	Oracle BI	The system must provide the ability to roll-up (summarize data) and drill-down (view details) in reports online.	Validated
A-25	Business Analytics	Platform	Oracle BI	The system must provide the ability to schedule the generation of reports at specific times.	Validated
A-26	Business Analytics	Platform	Oracle BI	The system must provide the ability to notify and distribute reports based on user specified criteria.	Validated
A-27	Business Analytics	Platform	Oracle BI	The system must provide the ability to organize reports into a shared list (library).	Validated
A-28	Business Analytics	Platform	Oracle BI	The system must restrict access to the shared list (library) or items within a shared list (library) to designated users.	Validated
A-30	Business Analytics	Platform	Oracle BI	The system must provide the ability to sort data within reports in multiple ways.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
A-31	Business Analytics	Platform	Oracle BI	The system must provide the ability to present data in graphical or chart format.	Validated
A-32	Business Analytics	Platform	Oracle BI	The system must provide the ability to limit report views based on user security / access rights.	Validated
A-33	Business Analytics	Platform	Oracle BI	The system must allow the user to export formatted reports from the system in industry standard formats.	Validated
A-34	Data Processing	Data Upload	Informatica	Allow uploads from authorized sources of data necessary to operate the Exchange	Validated
A-01	AUDIT: DATA QUALITY	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)	Validated
A-02	AUDIT:ELIGIBILITY DETERMINATION	Eligibility Determination	OneGate	Maintain data to produce a report of the outcomes of rules execution for all eligibility determinations (positive or negative) for appeals research and to analyze correctness of eligibility functionality.	Validated
A-19	BUSINESS ANALYTICS: SHOP, EE, PLAN MANAGEMENT	SHOP, EE,Plan Management	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 - Individual and employee financial data - Premium and CSR subsidy data - Enrollment data - Enrollee demographics	Validated
A-20	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The business analytics solution for the Exchange should not impact transactional database performance.	Validated
A-21	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to generate ad hoc reports.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
A-22	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to download and save report data to individual workstations and applications.	Validated
A-23	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to transmit reports to various designated recipients in a secure manner.	Validated
A-24	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to roll-up (summarize data) and drill-down (view details) in reports online.	Validated
A-25	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to schedule the generation of reports at specific times.	Validated
A-26	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to notify and distribute reports based on user specified criteria.	Validated
A-27	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to organize reports into a shared list (library).	Validated
A-28	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must restrict access to the shared list (library) or items within a shared list (library) to designated users.	Validated
A-30	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to sort data within reports in multiple ways.	Validated
A-31	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to present data in graphical or chart format.	Validated
A-32	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must provide the ability to limit report views based on user security / access rights.	Validated
A-33	BUSINESS ANALYTICS: PLATFORM	Platform	Oracle BI	The system must allow the user to export formatted reports from the system in industry standard formats.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
CACM-19	Consumer Assistance	Case Management - Administration	OneGate	The system must provide queries/reports to track and manage complaint workload, disposition, assignments and status	Validated
CAG-17	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The shall provide the capability to report complaint and appeals data in real time and on a historical basis.	Validated
CAG-25	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	The system shall collect and report on call center metrics for the purposes of identifying outreach and education opportunities	Validated
CAG-26	Consumer Assistance	Outreach / Education	Siebel Public Sector CRM	The system shall collect and report on website usage metrics including standard analytic metrics	Validated
CAG-27	Consumer Assistance	Outreach / Education	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	Validated
CAG-28	Consumer Assistance	Outreach / Education	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.	Validated
CAG-43	Consumer Assistance	Reporting	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.	Validated
CAG-44	Consumer Assistance	Reporting	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, fair hearing, grievances.	Validated
CAG-45	Consumer Assistance	Reporting	Siebel Public Sector CRM	The system shall have the ability to extract data in user friendly formats, such as Excel.	Validated
CAN-08	Consumer Assistance	Navigators	OneGate	Track the number of persons assisted by each Navigator on a monthly basis and produce detailed reports on such activity.	Duplicate
CAN-09	Consumer Assistance	Navigators	OneGate	Generate reports by Navigator; determining effectiveness by community, population, enrollment.	Duplicate
CAN-10	Consumer Assistance	Navigators	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.)	Validated
EN-36	Eligibility and Enrollment	Periodic Reporting	Oracle BI	Periodically and on an ad hoc basis provide electronic report to issuers about individual QHP enrollment data	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EN-38	Eligibility and Enrollment	Periodic Reporting	Oracle BI	Generate report of periodic issuer reconciliation to CMS	Validated
EN-39	Eligibility and Enrollment	Periodic Reporting	OneGate	Generate annual report to individual about QHP enrollment	Deferred
EN-40	Eligibility and Enrollment	Periodic Reporting	Oracle BI	Generate annual report to IRS about QHP enrollment	Deferred
PM-053	Plan Management	Evaluate QHP Issuer Application	TBD	Provide the ability to compile Issuer and product plan application evaluation results	Deferred
PM-101	Plan Management	Collect and Aggregate Plan Data	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: - Issuer data - Plan data including - Benefits structure - rates - enrollment	Validated
PM-104	Plan Monitoring	Monitor Issuer/Plan Compliance	TBD	Provide analytical queries and reports to analyze plan compliance and monitoring data	Deleted
PM-106	Plan Monitoring	Monitor Issuer/Plan Compliance	TBD	Provide the ability to analyze, display and report on performance data provided by Issuers	Deferred
PM-134	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Provide queries/reports to track and manage complaint workload, disposition, assignments and status	Validated
PM-135	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Provide sorts/reports/queries to support summarizing and analyzing complaints and complaint trends by a variety of complaint data attributes.	Validated
PM-136	Plan Management	Maintain Operational Data	Siebel Public Sector CRM	Publish approved complaint data summaries on the Exchange web portal for customer review , and to support transparency.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-157	Plan Management	Maintain Operational Data	TBD	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	Deferred
PM-158	Plan Management	Maintain Operational Data	TBD	The system must provide analytic tools/reports/queries to support determining Issuer/plan compliance with Exchange rules/policy	Deleted
PM-159	Plan Management	Maintain Operational Data	TBD	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.	Deleted
PM-160	Plan Management	Maintain Operational Data	OneGate	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.	Validated
PM-170	Plan Management	Maintain Operational Data	TBD	Provide tools/sorts/reports/queries to support summarizing and analyzing transparency and quality data	Validated
RP-01	Reporting	Business Analytics	Oracle BI	Provide a business analytics solution for the Exchange that will use a data warehouse for business intelligence, predictive analytics, and reporting.	Validated
RP-02	Reporting	Business Analytics	Oracle BI	Enable ad hoc query and reporting capability by authorized users	Validated
RP-03	Reporting	Business Analytics	Oracle BI	Store and recall saved queries created by authorized users	Validated
RP-04	Reporting	Business Analytics	Oracle BI	Track and maintain history of all ad hoc queries and reports run within the system	Validated
RP-05	Reporting	Business Analytics	Oracle BI	The data warehouse must, at a minimum, include the following dimensions: - Demographic dimension - Geographic dimension (including the entire State of VT)	Validated
RP-06	Reporting	Eligibility and Enrollment	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.	Duplicate

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
RP-07	Reporting	Financial Management	Premium Provider / OneGate / other approach	Provide summary reporting tools to the Exchange to be able to support reporting to various stakeholders on: plans, benefits, plan rates, premium costs, any administrative costs if known; issuer information; plan enrollment information	Validated
RP-08	Reporting	Financial Management	Oracle BI	Provide Exchange Enrollee Data to Risk Adjustment Entity	Deleted
RP-09	Reporting	Financial Management	Oracle BI	Generate Monthly Report on Individual Enrollment in Qualified Health Plan	Validated
RP-10	Reporting	Financial Management	Oracle BI	Generate report of Individual Premium Payment History to CMS	Validated
RP-11	Reporting	Financial Management	Oracle BI	Generate and Send Enrollment Discrepancy Reports to Issuer and CMS	Validated
RP-12	Reporting	Financial Management	Oracle BI	The Exchange will provide detail reports to support and reconcile the Annual Financial Report.	Validated
RP-13	Reporting	Plan Management	Oracle BI	Provide regular reporting on Plan Data to CMS. Schema should include: Enrollment, Cost and administrative per plan, Issuers, Plans, Benefit structure, Plan rates, Complaints	Validated
RP-14	Reporting	Plan Management	Oracle BI	Report on transparency and quality data to CMS	Validated
RP-15	Reporting	Plan Management	Oracle BI	Send notification of Change in Enrollment Availability to CMS	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
RP-16	Reporting	Plan Management	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 deductible - 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	Validated

RP-17	Reporting	Plan Management	Oracle BI	Provide periodic report to the Federal Data Services Hub to submit required data to CMS, but not limited to:
				- Issuer data
				- Plan data including
				  - Benefits structure
				  - rates
				  - enrollment
					Validated

RP-18	Reporting	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	Deleted
RP-19	Reporting	Plan Management	Oracle BI	The system must provide a Issuer performance indicator dashboard to aggregate performance data and display summary performance information by Issuer/Plan	Deferred

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
RP-20	Reporting	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	Validated
RP-21	Reporting	Plan Management	CGI Plan Management	Reporting on historical plan acceptance criteria	Validated
RP-22	Reporting	Plan Management	CGI Plan Management	Retain and report on periodic historical plan quality ratings as determined by the Exchange.	Validated
RP-23	Reporting	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	Validated
RP-24	Reporting	Plan Management	Siebel Public Sector CRM	The system must be able to track and manage complaints and consumer feedback about Issuers filed through the Exchange.	Validated
RP-25	Reporting	Plan Management	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	Validated
SH-131	Small Business	Update Employee Application	OneGate	Report employer contact information changes to the Issuer.	Validated
SH-194	Small Business	Employee Enrollment in QHP	OneGate	Prepare a communication to Issuer regarding employee enrollment in QHP	Validated
SH-197	Small Business	Employee Enrollment in QHP	OneGate	Provide notification to CMS regarding employee enrollment	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-205	Small Business	Disenroll Employee in QHP	OneGate	Prepare a notice to CMS with a minimum data set of information regarding an employee's disenrollment from a qualified health plan through the Exchange. This information is used for tax administration, as applicable.	Validated
SH-210	Small Business	Disenroll Employee in QHP	OneGate	If an employee has an involuntary disenrollment through the Exchange, prepare communication to the Issuer to terminate the employee.	Validated
SH-212	Small Business	Disenroll Employee in QHP	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.	Validated
SH-232	Small Business	Change Reporting	3rd Party Premium Processor	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.	Validated
SH-236	Small Business	Change Reporting	3rd Party Premium Processor	Report employee contact information changes to the Issuer.	Validated
WP-50	Web Portal	User Customization	OneGate	Provide a dashboard of key information and metrics for "super users" including electronic notice posting area.	Validated
NO-1	Notification	UX	OneGate	Users of the Exchange Web portal can view the history of all communication between the Exchange and the individual online	Validated
NO-2	Notification	Notification Engine	Thunderhead NOW	Provide the capability to target noticing at a family/household or individual level	Validated
NO-3	Notification	Notification Engine	Thunderhead NOW	Support the message body in a variety of formats including, but not limited to text, RTF, or HTML	Validated
NO-4	Notification	Notification Engine	Thunderhead NOW	Provide the capability to pass parameters to both the title and the body of the notification	Validated
NO-5	Notification	Notification Engine	Thunderhead NOW	Include graphics capability for notifications	Validated
NO-6	Notification	Notification Engine	Thunderhead NOW	Enforce size requirements on messages as defined by the Exchange	Validated
NO-7	Notification	Notification Engine	Thunderhead NOW	Recognize "opt-out" flags attached to individual records and suppress notifications to those individuals	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-8	Notification	Notification Engine	Thunderhead NOW	Recognize and "invalid e-mail" flag and suppress notifications to those addresses	Validated
NO-9	Notification	Notification Engine	Thunderhead NOW	Filter out and suppress live e-mails for notification test instances	Validated
NO-10	Notification	Notification Engine	Thunderhead NOW	Assign a notification ID (notification event) and include on all messages as determined by the Exchange	Validated
NO-11	Notification	Notification Engine	Thunderhead NOW	Support barcoding of outgoing notifications	Validated
NO-12	Notification	Notification Engine	Thunderhead NOW	Provide the capability to include both dynamic and static attachments	Validated
NO-13	Notification	Notification Engine	Thunderhead NOW	Allow for embedded links within notification message	Validated
NO-14	Notification	Notification Engine	Thunderhead NOW	Provide tools to manage e-mail "bouncebacks", including the ability to parse the "bounceback" message for actions	Validated
NO-15	Notification	Notification Engine	Thunderhead NOW	Provide the capability to include the message ID in the notification subject line	Validated
NO-16	Notification	Financial Management	Premium Processor / OneGate / other options	Notify Employer of Payment Discrepancy	Duplicate
NO-17	Notification	Financial Management	Premium Processor / OneGate / other options	Provide Invoices to Individuals	Duplicate
NO-18	Notification	Financial Management	Premium Processor / OneGate / other options	Provide notifications to employees of payment discrepancy from Small Business	Duplicate
NO-19	Notification	Financial Management	Premium Processor / OneGate / other options	Provide notification to individuals of payment discrepancy from Exchange	Duplicate
NO-20	Notification	Financial Management	Premium Processor / OneGate / other options	The Issuer invoice will be generated and a Notification sent to the Issuer.	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-21	Notification	Financial Management	Premium Processor / OneGate / other options	Communicate to the Exchange of the discrepancy.	Duplicate
NO-22	Notification	Financial Management	Premium Processor / OneGate / other options	Send notification of unpaid premiums to employers.	Duplicate
NO-23	Notification	Financial Management	Premium Processor / OneGate / other options	The invoice notification would include a link to login to the Exchange and make an electronic payment.	Duplicate
NO-24	Notification	Eligibility and Enrollment	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	Validated
NO-25	Notification	Eligibility and Enrollment	OneGate	Send notification for change in individual's Eligibility Status	Validated
NO-26	Notification	Eligibility and Enrollment	OneGate	When additional verification is required, provide on-screen notification to individual to supply additional verifications through the exchange.	Validated
NO-27	Notification	Eligibility and Enrollment	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.	Duplicate
NO-28	Notification	Eligibility and Enrollment	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.	Duplicate

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-29	Notification	Eligibility and Enrollment	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.	Validated
NO-30	Notification	Eligibility and Enrollment	OneGate	Prepare and provide communication to individuals about a mid-year plan decertification and notify need for plan selection / enrollment.	Validated
NO-31	Notification	Eligibility and Enrollment	OneGate	Prepare written and on-screen notification to individuals regarding eligibility for enrollment periods.	Validated
NO-32	Notification	Eligibility and Enrollment	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.	Duplicate
NO-33	Notification	Eligibility and Enrollment	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.	Duplicate
NO-34	Notification	Eligibility and Enrollment	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.	Validated
NO-35	Notification	Eligibility and Enrollment	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-36	Notification	Eligibility and Enrollment	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.	Validated
NO-37	Notification	Eligibility and Enrollment	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.	Validated
NO-38	Notification	Eligibility and Enrollment	OneGate	Provide electronic notification to CMS of the result of an individual's eligibility determination.	Duplicate
NO-39	Notification	Eligibility and Enrollment	Siebel Public Sector CRM	Generate a notification to CMS of any completed appeals decisions.	Validated
NO-40	Notification	Eligibility and Enrollment	OneGate	Send a formal, written notice to a individual's mailing address summarizing eligibility determination for individual exemption	Duplicate
NO-41	Notification	Eligibility and Enrollment	OneGate	Send an automated transaction individuals who have been determined as exempt or not exempt to CMS	Validated
NO-42	Notification	Eligibility and Enrollment	OneGate	Send a formal, written notice to a individual's mailing address summarizing eligibility determination for individual exemption	Duplicate
NO-43	Notification	Small Business	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.	Validated
NO-44	Notification	Small Business	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-45	Notification	Small Business	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	Validated
NO-46	Notification	Small Business	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.	Validated
NO-47	Notification	Small Business	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.	Validated
NO-48	Notification	Small Business	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.	Validated
NO-49	Notification	Small Business	OneGate	Produce a notice of annual open enrollment.	Validated
NO-50	Notification	Small Business	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).	Validated
NO-51	Notification	Small Business	Siebel Public Sector CRM	Generate a formal written notice informing an employer of the details of an appeal decision.	Validated
NO-52	Notification	Small Business	Siebel Public Sector CRM	Generate a notification to CMS of any completed appeals decisions.	Validated
NO-53	Notification	Small Business	OneGate	Generate a notification to an employer regarding the employer's adjusted eligibility determination based on the employer's Exchange eligibility appeal decision.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-54	Notification	Small Business	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	Validated
NO-55	Notification	Small Business	OneGate	Generate written and on-screen notification of the result of an employee's eligibility determination	Validated
NO-56	Notification	Small Business	OneGate	Produce an automated and real-time, electronic notification of plan selection.	Validated
NO-57	Notification	Small Business	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.	Validated
NO-58	Notification	Small Business	OneGate	If an employee initiates a voluntary disenrollment through the Exchange, produce an electronic notification to the Issuer to disenroll the employee.	Validated
NO-59	Notification	Small Business	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.	Validated
NO-60	Notification	Small Business	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.	Validated
NO-61	Notification	Small Business	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.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-62	Notification	Small Business	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.	Validated
NO-63	Notification	Small Business	OneGate	Produce a notice of annual open enrollment.	Duplicate
NO-64	Notification	Small Business	OneGate	Process notification notifying employer of coverage for employees. Also, communicate any next steps required by the employer.	Validated
NO-65	Notification	Small Business	OneGate	Provide capability to generate a notification to CMS of any completed appeals decisions.	Duplicate
NO-66	Notification	Small Business	OneGate	Generate a notification to an employee regarding the employee's adjusted eligibility determination based on the employee's Exchange eligibility appeal decision.	Validated
NO-67	Notification	Small Business	OneGate	Prepare and send communication to the employer regarding changes to the Employer's worksite locations.	Validated
NO-68	Notification	Small Business	OneGate	Prepare and send communication to the employer regarding changes to the employer's employee roster.	Validated
NO-69	Notification	Small Business	OneGate	Prepare and send communication to the employee regarding changes to the Employee contact information.	Validated
NO-70	Notification	Small Business	OneGate	Report employee contact information changes to the Issuer.	Validated
NO-71	Notification	Small Business	OneGate	Prepare and send communication to the employee regarding changes to the employee's account due to a Qualifying Event.	Validated
NO-72	Notification	Small Business	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.	Validated
NO-73	Notification	Small Business	OneGate	Process notification notifying employer of coverage for employees. Also, communicate any next steps required by the employer.	Duplicate
NO-74	Notification	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	Deleted
NO-75	Notification	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	Deferred

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-76	Notification	Plan Management	CGI Plan Management	Produce electronic and paper notices to Issuers when a plan is not renewed to be in the Exchange	Deleted
NO-77	Notification	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.	Deleted
NO-78	Notification	Plan Management	CGI Plan Management	Upon request, generate and send non-renewal notices to Issuers about the plans not be renewed.	Deleted
NO-79	Notification	Plan Management	CGI Plan Management	Upon request, generate and send electronic decertification notices to Issuers about the plans to be decertified.	Deleted
NO-80	Notification	Plan Management	CGI Plan Management	Upon request, generate and send letter (mail) decertification notices to Issuers about the plans to be decertified.	Deleted
NO-81	Notification	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.	Deleted
NO-82	Notification	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.	Validated
NO-83	Notification	Plan Management	CGI Plan Management	Recertify the plan and notify issuers consistent with the initial certification process.	Deleted
NO-84	Notification	Plan Management	CGI Plan Management	Update CMS with plan certified plan information consistent with the initial certification process	Validated
NO-85	Notification	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.	Validated
NO-86	Notification	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.	Deleted
NO-87	Notification	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.	Deleted
NO-88	Notification	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	Deleted
NO-89	Notification	Plan Management	CGI Plan Management	Provide the ability to provide submitted rate and benefit data to the Insurance Division system electronically	Deleted

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-90	Notification	Plan Management	CGI Plan Management	Registered Navigators/Brokers must be able to subscribe to Exchange notifications	Validated
NO-91	Notification	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	Duplicate
NO-92	Notification	Plan Management	CGI Plan Management	Produce electronic or paper notices to Issuers when a plan is not renewed to be in the Exchange	Duplicate
NO-93	Notification	Plan Management	CGI Plan Management	Produce electronic or paper notices to Issuers when a plan is not decertified from Exchange	Deleted
NO-94	Notification	Plan Management	CGI Plan Management	Record the plan or issuer decertification event and status information, including date, reason/rationale.	Deleted
NO-95	Notification	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	Deleted
NO-96	Notification	Plan Management	CGI Plan Management	Produce electronic notification to CMS when an Issuer/plan is not renewed or is decertified from the Exchange	Validated
NO-97	Notification	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.	Duplicate
NO-98	Notification	Plan Management	CGI Plan Management	Upon request, generate and send non-renewal notices to Issuers about the plans not be renewed.	Duplicate
NO-99	Notification	Plan Management	CGI Plan Management	Upon request, generate and send electronic decertification notices to Issuers about the plans to be decertified.	Duplicate
NO-100	Notification	Plan Management	CGI Plan Management	Upon request, generate and send letter (mail) decertification notices to Issuers about the plans to be decertified.	Duplicate
NO-101	Notification	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.	Duplicate
NO-102	Notification	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.	Duplicate
NO-103	Notification	Plan Management	CGI Plan Management	Generate re-amendment notification and information storage consistent with the initial certification amendment process.	Deferred
NO-104	Notification	Plan Management	CGI Plan Management	Update CMS with plan certified plan information consistent with the initial certification process	Duplicate

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
NO-105	Notification	Plan Management	CGI Plan Management	Provide notices to be sent to plan consumers if a provider network change requires consumer notification.	Deleted
NO-106	Notification	Plan Management	CGI Plan Management	Notify authorized Exchange users when an Issuer has updated any Issuer, plan and provider data	Deleted
NO-107	Notification	Plan Management	CGI Plan Management	Authorized Exchange users must automatically receive notification that an enrollment request has been received.	Deleted
NO-108	Notification	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.	Deleted
NO-109	Notification	Plan Management	CGI Plan Management	Approval of the enrollment change request must generate an electronic notification to Exchange issuers indicating the plan enrollment status	Validated
NO-110	Notification	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	Validated
NO-111	Notification	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	Validated
NO-112	Notification	Plan Management	CGI Plan Management	Approval or disapproval of the enrollment change request must send notification to the requesting Issuer.	Validated
PM-175	Plan Management	Process Change in Plan Enrollment Availability	Manual	Provide automatic notification to authorized Exchange users indicating that an enrollment request has been received.	Duplicate
PM-178	Plan Management	Process Change in Plan Enrollment Availability	Manual	Upon approval of the enrollment change request, generate an electronic notification to Exchange Issuers indicating the plan enrollment status	Duplicate

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
PM-179	Plan Management	Process Change in Plan Enrollment Availability	TBD	Upon approval of the enrollment change request, generate an electronic notification to registered Navigators/Brokers indicating the plan enrollment status	Duplicate
PM-181	Plan Management	Process Change in Plan Enrollment Availability	Manual	Upon approval or disapproval of the enrollment change request, generate notification to the requesting Issuer.	Duplicate
CAG-18	Consumer Assistance	Complaints / Appeals	Siebel Public Sector CRM	The system shall provide notifications to the appropriate parties upon the following key events in the complaint/appeal process: - Receipt of complaint/appeal - Status Change - Resolution	Validated
SH-122	Small Business	Appeal Small Business Eligibility Decision	OneGate	Generate a notification to CMS of appeals decisions in which a renewal is denied.	Validated
SH-126	Small Business	Periodic Reporting and Reconciliation	OneGate	Prepare and send communication to the employer regarding changes to the employer's employee roster.	Validated
SH-128	Small Business	Change Reporting/Periodic Reporting	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 Small Business Tax Credit.	Deferred
SH-132	Small Business	Update Employee Application	OneGate	Prepare and send communication to the employer regarding changes to the Employer contact information.	Validated
SH-136	Small Business	Renew / Redetermine Employer Participation	OneGate	Provide notification to employers when annual election period is approaching	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-137	Small Business	Renew / Redetermine Employer Participation	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.	Deleted
SH-140	Small Business	Renew / Redetermine Employer Participation	OneGate	Prepare and send communication to the employer regarding changes to the Employer's worksite locations.	Validated
SH-150	Small Business	Determine Employee Eligibility	OneGate	Inform employees that may be eligible for subsidized coverage at a lower premium and allow for an individual eligibility determination.	Validated
SH-191	Small Business	Employee Selects QHP	OneGate	Produce an automated and real-time, electronic notification of plan selection.	Validated
SH-196	Small Business	Employee Enrollment in QHP	OneGate	Provide notification of successful enrollment to employee	Validated
SH-200	Small Business	Disenroll Employee in QHP	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.	Validated
SH-201	Small Business	Disenroll Employee in QHP	OneGate	If an employee initiates a voluntary disenrollment through the Exchange, produce an electronic notification to the Issuer to disenroll the employee.	Validated
SH-207	Small Business	Disenroll Employee in QHP	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.	Validated
SH-208	Small Business	Disenroll Employee in QHP	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.	Duplicate
SH-213	Small Business	Renew Employee QHP Participation	OneGate	Provide automatic renewal notice to employees	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
SH-217	Small Business	Update Employee Application / Renew Employee QHP Participation	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.	Validated
SH-219	Small Business	Renew Employee QHP Participation	OneGate	Produce a notice of annual open enrollment.	Validated
SH-220	Small Business	Renew Employee QHP Participation	OneGate	Produce notification to employees regarding the number of days left for open enrollment.	Validated
SH-233	Small Business	Change Reporting	OneGate	Prepare and send communication to the employee regarding changes to the employee's account due to a Qualifying Event.	Validated
SH-237	Small Business	Change Reporting	OneGate	Prepare and send communication to the employee regarding changes to the Employee contact information.	Validated
EL-16	Eligibility and Enrollment	Individual Exemption from Responsibility	OneGate	Send real-time, automated notifications and written notices to Individuals of CMS determinations of exemption status, and update individual accounts accordingly.	Validated
EL-17	Eligibility and Enrollment	Individual Application & Submit Update	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.	Validated
EL-22	Eligibility and Enrollment	Individual Application & Submit Update	CGI	Send notifications to the Individuals regarding the enrollment process and the status of their application.	Validated
EL-20	Eligibility and Enrollment	Individual Application & Submit Update	CGI	Send notifications to the Individuals who have not completed their applications informing them of the expiration date.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
EL-19	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Send notifications to the Individuals, alerting them to submit required eligibility or verification information.	Duplicate
EL-21	Eligibility and Enrollment	Individual Application & Submit Update	OneGate	Send notifications to the Individuals, Exchange Staff, Brokers, and Navigators of changes to Individuals' applications.	Validated
EL-51	Eligibility and Enrollment	Participation in the Exchange	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.	Validated
EN-8	Eligibility and Enrollment	Plan Selection	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.	Validated
EN-34	Eligibility and Enrollment	Enrollment	OneGate	Prepare written notification to individuals regarding eligibility for enrollment periods.	Duplicate
EL-56	Eligibility and Enrollment	Individual Eligibility Determination-Verification	OneGate	Generate online or written requests to Individuals for additional documentation and allow electronic submission of documents, link to accounts, and track follow up activities.	Validated
WP-1	Web Portal	Design	OneGate	Design based on Enrollment 2014 UX project	Met
WP-2	Web Portal	Design	OneGate	Provide content specific help on screen for users	Met
WP-3	Web Portal	Design	OneGate	Provide additional language support features. At a minimum, the system should provide language "flag" icons to direct consumes in their native language to Navigator and/or Translation services	Validated
WP-4	Web Portal	Design	Siebel Public Sector CRM	Persist telephone support options on all Portal views	Met
WP-4A	Web Portal	Design	Siebel Public Sector CRM	Persist live chat support options on all Portal views	Deferred
WP-5	Web Portal	Design	OneGate	Provide trained business user portal content management capabilities	Met
WP-6	Web Portal	General	OneGate	Display general information about the state's health and human services programs publicly for all users to view without requiring a login.	Validated

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
WP-7	Web Portal	General	OneGate	Display and provide browsing capabilities on the various health options and plans available to users without requiring a login.	Validated
WP-8	Web Portal	General	OneGate	Provide robust search capability for information contained on the portal without requiring a login.	Met
WP-9	Web Portal	General	OneGate	Provide capability for users to search for Navigators using a variety of criteria without requiring a login.	Validated
WP-10	Web Portal	General	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.	Validated
WP-11	Web Portal	General	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.	Met
WP-12	Web Portal	General	OneGate	Provide an expedited expert level pre-screening function to Navigators, brokers, call center staff, and caseworkers.	Validated
WP-13	Web Portal	General	OneGate	Accept input from Navigators, caseworkers, Call Center staff and customers necessary for pre-screening.	Validated
WP-14	Web Portal	General	OneGate	Display the results of the pre-screening assessment of eligibility to Navigators, caseworkers, call center staff, and customers.	Validated
WP-15	Web Portal	General	OneGate	Provide the ability to flag any information or situations that require more detailed information and direct individuals for further assistance.	Validated
WP-16	Web Portal	General	OneGate	Support additional data-gathering regarding user experience with QHPs and/or quality of care (i.e. surveys, questionnaires, etc.)	Validated
WP-17	Web Portal	Identity	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.)	Met
WP-18	Web Portal	Identity	OneGate	Provide verified 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)	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
WP-19	Web Portal	Enrollment	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	Validated
WP-20	Web Portal	Enrollment	OneGate	Enable individual users to compare plans based on factors such as -Premium/Expense (Monthly Cost, Annual Out of pocket expense, Monthly premium) - Carrier - Plan type (HMO, PPO, POS, PCCM) - Product Type (e.g. Vision, Dental, etc. - Quality Rating (0 - 4)	Met
WP-20a	Web Portal	Enrollment	OneGate	Enable individual users to compare plans based on factors such as - Medal Rating - Benefit Structure - Member-provided feedback rating	Deferred
WP-21	Web Portal	Enrollment	OneGate	Provide multiple summary and detail levels of plan comparison information	Met
WP-22	Web Portal	Enrollment	OneGate	Enable users to look up the providers that are affiliated with specific plans and affiliation type (i.e. Tiered PPO model).	Validated
WP-23	Web Portal	Enrollment	Plan Management	Provide ability for Issuers to upload supporting documentation to the plan selection tool	Validated
WP-24	Web Portal	Enrollment	OneGate	Provide a plan selection recommendation engine or wizard that can filter initial results based upon additional user preference and input.	Validated
WP-25	Web Portal	Enrollment	OneGate	Provide capability for users to download additional supporting plan documentation as provided by the Issuer	Validated
WP-26	Web Portal	Enrollment	OneGate	Provide calculator functionality for individuals to estimate their premiums including potential premium tax credit subsidies and cost sharing reductions	Validated
WP-27	Web Portal	Eligibility	OneGate	Provide a dynamic application entry engine to collect information required to determine eligibility for health and human service programs. The system shall tailor the application process based upon user response to questions.	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
WP-28	Web Portal	Eligibility	OneGate	Provide a progress bar to show users where they are in the application process	Met
WP-29	Web Portal	Eligibility	OneGate	Enable individual users to submit information for eligibility, for example: - SSN - Address - Date of birth - Name - Household income	Met
WP-30	Web Portal	Eligibility	OneGate	Provide status of eligibility request received from the eligibility service	Validated
WP-31	Web Portal	Eligibility	OneGate	Display eligibility results received from the eligibility service	met
WP-32	Web Portal	Eligibility	OneGate	Enable individual users to apply for benefits eligibility using alternate income verification (i.e. paper verification).	Validated
WP-33	Web Portal	Enrollment	OneGate	Enable individual users to enroll in a plan which they have selected	Met
WP-34	Web Portal	Enrollment	OneGate	Enable individual users to reenroll (renew) in a plan which they have selected	Validated
WP-35	Web Portal	Financial Management	OneGate	Allow users to set up payment options for their selected plan(s)	Validated
WP-36	Web Portal	Financial Management	OneGate	Allow users to make recurring and scheduled electronic premium payments through the Exchange portal	Validated
WP-37	Web Portal	Financial Management	OneGate	Allow authorized users the ability to view their payment histories on the Web Portal	Validated
WP-38	Web Portal	Small Business	OneGate	Enable Employer to set up SHOP plan selection(s)	Met
WP-39	Web Portal	Small Business	OneGate	Enable Employees to compare available SHOP plans	Met
WP-40	Web Portal	Small Business	OneGate	Enable Employees to enroll or unenroll in SHOP plan	Met
WP-41	Web Portal	Small Business	OneGate	Allow employers to set up payment options for premiums	Validated
WP-42	Mobile Web Portal	Enrollment, Financial Management	OneGate	Enable users of all plans to view their enrollment and payment status, plan details, and notification history	Met

© Copyright 2013, CGI

Ref Code	Category	Sub Category	Application or Module	Requirement Description "The system shall..."	Current Disposition
WP-43	Mobile Web Portal	Eligibility	OneGate	Enable users to upload eligibility documents using their camera equipped mobile device	Deferred
WP-44	Support Intranet	Security	OneGate	Provide role based access to Exchange Portal content	Met
WP-45	Web Portal	Administration	OneGate	Provide role based portal administration function	Met
WP-46	Web Portal	Financial Management	OneGate	View Invoice and invoice details for Individual, Employer and Issuers	Validated
WP-47	Web Portal	Financial Management	OneGate	Make electric payment for Individual, Employer, and Issuer	Validated
WP-48	Web Portal	Financial Management	OneGate	View notification history for Individuals, Employers, and Employees	Validated
WP-49	Web Portal	User Customization	OneGate	Provide customizable portal views and functionality based on user role for "super users" (e.g. Navigator, Broker, caseworker, etc.)	Validated
WP-51	Web Portal	User Customization	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.	Deferred
WP-52	Web Portal	User Customization	OneGate	Allow SHOP owners access to the Exchange through a custom portal and add or manage health plan options for their employees.	Met
WP-53	Web Portal	User Customization	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.	Met

© Copyright 2013, CGI

Statement of Work No. 4

This Statement of Work No. 4 ("**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 and July __, 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.

Pursuant to Statement of Work No. 1 to the MSA, effective as of December 17, 2012, as amended ("**SOW #1**"), SOV and the Supplier agreed to develop and refine the scope of the hosting services to be delivered by Supplier under SOW #1. As a result of such scope refinement, SOV and Supplier agreed to separate the hosting services from the other IT Services being providing under SOW #1 and therefor as of the date hereof are amending and restating SOW #1 and entering into this SOW, pursuant to which the hosting services will be provided.

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 IT Services based on the Non-Functional Requirement Traceability Matrix ("**Non-Functional RTM**") attached here as Schedule A to this SOW and incorporated herein by reference and as further described in Exhibit I, Exhibit D, Exhibit J and the MSA The Services provided under this SOW will be referred to as the "Hosting Services." Additional assumptions regarding the scope of the Hosting Services is provided in the three diagrams attached as Schedule B to this SOW and incorporated herein by reference. The Hosting Services will be provided in a CGI environment that conforms in all respects the requirements of the Non-Functional RTM and the MSA, except that SOV agrees that this environment is a shared service environment and not a dedicated hosting environment.

B. Location of Services.

Supplier provided Hosting Services will be located at the followingdata center sites.

Primary	CGI Phoenix Data Center	10007 South 51st Street Phoenix, AZ 85044
Secondary	CGI Philadelphia Data Center	3rd floor hosting - CGI Technologies. 1500 Spring Garden St Philadelphia, PA 19130

C. Deliverables and Work Product.

Upon Go-Live of the System (as defined in Exhibit D), Supplier will provide a monthly report of the Service Level Agreement results as detailed in Exhibit D. Additional details regarding Work Product are documented in the SOW#1 Project Management Plan ("**PMP**").

D. Milestone Schedule

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

E. Acceptance Criteria and Process.

The acceptance criteria for Hosting Services is set forth in the PMP.

F. Supplier Personnel.

Operations Manager, Robert Carlin is Key Personnel. The process for approval of Supplier Personnel in Key Supplier Positions is described in the MSA.

G. Supplier Resources.

Description of Supplier Resources is set forth in the PMP.

H. SOV Roles and Responsibilities.[1]

1. The SOV is responsible for appointing a dedicated full-time SOV resource to establish and manage a team to work with Supplier in connection with the Hosting Services and provide for timely completion of the SOV's responsibilities.
2. 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 for the operation of State of Vermont agency interfaces and insurance carrier interfaces.
3. The SOV is responsible for providing space and furnishings in an SOV facility for an agreed upon number of Supplier Personnel. Supplier is responsible for providing computer equipment needed for its staff.
4. The SOV will provide badge access for agreed upon Supplier Personnel to identified locations for the Statement of Work Term as long as such Supplier Personnel subject to the terms and conditions of the MSA, including without limitation that such Supplier Personnel meet the SOV security requirements necessary to provide a badge.
5. The SOV will provide wireless, internet connectivity to agreed upon Supplier Personnel staff at the SOV site.
6. Proprietary Materials: SOV will provide licenses for Oracle products to be implemented on SOV's behalf in the Hosting Services for the Exchange.[2]

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 executing this SOW 2, 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, if any, 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. PROJECT MANAGERS.

The Operations Manager (as defined in Section F above) is the Project Manager for this SOW.

---

4. STAFF.

A. Subcontractors.
Supplier has engaged Exeter Consulting (and its affiliates) to configure the OneGate product. Supplier has engaged Oracle Consulting Services to configure the Oracle products. The scope of the subcontractor configuration work is set forth in the PMP and the RTM.

---

5. SOFTWARE.

A. Third Party Software provided by Supplier
Subject to the terms and conditions of the MSA, Supplier will procure the Third Party Software for SOV (the licenses for which will be directly between Supplier and the respective third party vendor) listed as Third Party Software in Exhibit L (Pricing) in Section 5.2.9.4 of Part 2.

B. Third Party Software provided by SOV.

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

6. HARDWARE.

At no additional charge to SOV, Supplier is responsible for the procurement, operation and maintenance of all Equipment used by or for the benefit of SOV in connection with the Hosting Services or used by or for the benefit of Supplier to provide or support the provision of the Hosting Services.

7. THIRD PARTY CONTRACTS.

Not applicable to this SOW

8. SERVICE LEVELS.

The Service Levels and Service Level Credits in Exhibit D attached to the MSA apply to the Hosting Services.

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

As required by the MSA.

10. FORECASTING

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

11. FACILITIES TO BE PROVIDED BY SUPPLIER.

Not applicable.

12. ASSUMPTIONS.

Not applicable to this SOW.

13. OPTIONAL SERVICES.

A. Not applicable to this SOW.

14. OTHER SERVICES.

A. Not applicable to this SOW

15. CHARGES AND PASS-THROUGH EXPENSES.

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

16. ADDITIONAL TERMS.

A. Not applicable.

Agreed to and accepted by:

CGI Technologies and Solutions Inc. (CGI)	State of Vermont
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

SCHEDULE A

Non-Functional RTM

[see attached]

SCHEDULE B

Hosting Environments Diagrams

[see attached]

State of Vermont Enterprise Architecture

Non-Functional Requirements Traceability Matrix (RTM)

Table of Contents

		Code	Description	Tab	Order
	Table of Contents		Table of Contents	Table of Contents	1
	General		Change Log for this spreadsheet.	Change Log	2
			Definitions	Definitions	3
	Hosting Services	H1	Data Center	H1 Data Center	4
		H1A	TIA 942 Data Center Standards	H1A TIA 942	5
		H2	Infrastructure	H2 Infrastructure	6
		H3	Networking	H3 Networking	7
		H4	Backup Recovery	H4 Backup Recovery	8
		H5	Capacity & Performance Mgmt	H5 Capacity & Performance	9
		H6	Configuration Management	H6 Configuration	10
		H7	Release Management	H7 Release	11
		H8	Monitoring Management	H8 Monitoring	12
		H9	Service Continuity Management	H9 Continuity	13
		H10	Refreshes and Lifecycle	H10 Refreshes	14
		H11	Maintenance and Operations	H11 M&O	15
		H12	Governance	H12 Governance	16
		H13	Service Level Agreement	H13 SLA	17
	Security/Privacy	S1	Security Summary	S1 Security	18
		S2A	General Security Tab 1	S2A General Security	19
		S2B	General Security Tab 2	S2B General Security	20
		S3	Federal Security	S3 Federal Security Service	21
		S4A	NIST 800-53 Summary	S4A NIST 800 Series Summary	22
		S4B	NIST 800-53 Details	S4B NIST 800 Series Detail	23
		S5	HIPAA	S5 HIPAA	24
		S6	PHI and Privacy	S6 PHI and Privacy	25
		S7	IRS 1075	S7 IRS 1075	26
		S8	PCI-DSS	S8 PCI	27
	Solution	SLN1	Service Oriented Architecture	SLN1 SOA	28
		SLN2	Audit	SLN2 Audit	29
		SLN3	Business Intelligence & Extract Transform and Load (ETL)	SLN3 BI & ETL	30
		SLN4	Master Data Management and Integration	SLN4 MDM & INT	31
		SLN5	Interfaces	SLN5 Interfaces	32
		SLN6	Medicaid Information Technology Architecture (MITA)	SLN6 MITA	33
		SLN7	Rules Engine and Standards	SLN7 Rules	34
		SLN8	Portal	SLN8 Portal	35
		SLN9	Enterprise Content Management (ECM)	SLN9 ECM	36
		SLN10	Database Management System (DBMS)	SLN10 DBMS	37
		SLN11	Application Architecture	SLN11 APP Arch	38
		SLN12	Useability	SLN12 Useability	39
		SLN13	Software Requirements and useage	SLN13 Software	40
		SLN14	Users of the Solution and their touch points	SLN14 Actors	41
		SLN15	ACCESS Remediation SOW	SLN15 ACCESS SOW	42
	Target Environment Review	ENV1	see Production Environments Technical Architecture Model	[Hosting] VT HSEP HBE Environments - Physical and Virtual Architecture for Environments v3 05242013 MMorey.pdf	
		ENV2	see Non-Production Environments Technical Architecture Model	[Hosting] VT HSEP HBE Environments - Physical and Virtual Architecture for Environments v3 05242013 MMorey.pdf	
	WAN Connectivity	WAN1	see WAN Connectivity Schematic	[Hosting] SOV WAN Network diagram 03_22_13 v6 - Chase ep pref vendor update.pdf	

Date	Author	Version	Change Reference
	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.
14-Mar-2013	MMOREY	V3.1	Removed Y/N for clarity as these are non functional requirements. Unified/Clarified requirements where CGI had indicated they could meet but with exception. Modified WAN connectivity diagram to include premium processor.
16-Apr-2013	Chad Loseby		WORKING COPY. Merged in changes from Chad's ChangeLog.
16-Apr-2013	Paul Haigh	V4.0	WORKING COPY. Merged in changes from Paul's ChangeLog.
17-Apr-2013	Chad Loseby	V4.1	WORKING COPY. Seel SLN15 - Merged in requirements from ACCESS Remediation SOW NFR RTM
17-May-2013	Paul Haigh	V5.0	Removed this from the Definitions Tab: "XXX This is the document we are working on."
17-May-2013	Paul Haigh	V5.1	Replaced "Project teams (vendor-supplied or otherwise)" with "Supplier".
21-May-2013	Paul Haigh	v5.2	Removed: H2.1.21,Infrastructure,General Hosting Provider will build Customers private cloud utilizing dedicated physical and virtual separation and components.
22-May-2013	Paul Haigh	v5.3	Made change to "H11.1.34". Removed "During the maintenance period, ".
24-May-2013	Paul Haigh	v5.4	Modified Table of Contents to include Diagrams for Hosting and Wan Design.

18-Jun-2013	Eddy Paul	v5.5	Deleted H2.1.2 Verbiage modified as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	Modified H2.1.17 Verbiage modified as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	Modified H2.1.18 Verbiage modified as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	Modified H2.1.21 Verbiage modified as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	Modified H4.1.4 Verbiage modified as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	Modified H4.1.5 Verbiage modified as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	Modified H4.1.17 Please see 28.5 miles as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	Modified H11.1.12 through H11.1.14 to read H9.1.12 through H9.1.14 (H9 Continuity tab)
18-Jun-2013	Eddy Paul	v5.5	Modified H9.1.12 Verbiage modified as per discussion 6/21/13
18-Jun-2013	Eddy Paul	v5.5	H7.1.3 Verbiage modified as per discussion 6/21/13
21-Jun-2013	Eddy Paul	v5.5	H1A T1A3.6 outstanding question
21-Jun-2013	Rob Ball	v5.6	Removed SLN4.1.72, SLN4.1.73 and SLN4.1.74. These are functional requirements
21-Jun-2013	Rob Ball	v5.6	SLN3.1.3 removed text "Suggest the following change"
21-Jun-2013	Rob Ball	v5.6	SLN5.1.1 removed -- self reference requirement to itself
21-Jun-2013	Rob Ball	v5.6	SLN51.32 removed. This is a functional requirement
21-Jun-2013	Rob Ball	v5.6	SLN7.1.34 removed text "while maintaining compliance with CMS rules."
21-Jun-2013	Rob Ball	v5.6	SLN10.1.19 removed text "Note: Vermont needs to validate # of months"
21-Jun-2013	Rob Ball	v5.6	SLN13 Software -- changed Siebel Email/Web Offer Designer, Siebel Email Marketing Server, Siebel Campaign Management, Siebel Web Marketing, Siebel Marketing Server entries to indicate Vermont ULA and CGI Validation
23-Jun-2013	Paul Haigh/Rick Ketchem/Rob Ball	v5.7	SLN15.1.15 Deleted (covered elsewhere): - NIST 800-53A and NIST 800-53 rev3 Moderate baseline - IRS pub 1075, which points back to NIST 800-53 rev 3 - NIST 800-53A rev1 guidance (http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf) and Harmonized Security and Privacy Framework. - CMS requirements, which points back to NIST 800-53 rev3 moderate baseline
23-Jun-2013	Paul Haigh/Rick Ketchem/Rob Ball	v5.7	TIA.3.6 removed requirement

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.
	Agent	Agent can be the term substituted for the Hosting Provider.
	Agreement	Agreement is defined as: the Master Service Agreement between SOV and CGI, and its supporting exhibits, addendums, and statements of work
	Anticipated Peak Workload	Anticipated Peak Workload means target or goal workload for the Hosting Environment during testing.
	Application	Application is defined as: a specific instance of computer software, purchased or developed, which performs essential functions
	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 Server	An Application Server is a software framework dedicated to the efficient execution of procedures (programs, routines, scripts)
	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.
	Availability Management	Availability Management is defined as: the measurement and management of infrastructure, including measurement of service failures and the time taken to resume service.
	Availability Plan	The Availability Plan is the plan that detils the availability of both the services provided by the Hosting Provider.
	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.
	Bandwidth	Bandwidth is defined as: the amount of traffic to be carried through a network.
	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.
	Capacity Plan	Capacity Plan is defined as: Documentation of how the Solution's capacity requirements were calculated, including all formulas and actual calculations, and how the requirements will be met, managed, monitored, and resolved.
	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 Management	Configuration Management is defined as: the process of identifying, recording, and reporting of Infrastructure components (hardware, software, and associated documentation), including but not limited to their versions, constituent components, and relationships.
	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.
	Continental United States (CONUS)	Continental United States (CONUS) refers to the continental or contiguous 48 states including DC. It excludes Hawaii, Alaska, and any other territory.
	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.
	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" shall refer to the Hosting Provider Data Center unless specified otherwise
	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 Data Service Hub	The Federal Data Service Hub is the electronic interface being created by the Center or Medicare &Meidaid Services (CMS) that will serve as an information hub to provide one connection to the common federal data sources (including but not limited to SSA, IRS, DHS) needed to verify consumer application information for income, citizenship, immigration status, access to minimum essential coverage, etc.

	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.
	Federal Tax Information (FTI)	Federal Tax Information (FTI) is defined as: federal tax returns, and information contained on said tax returns
	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.
	Governance	Governance is the action or manner of governing. Governance Services refers to the process whereby the Hosting Provider provides expertise in the area Governance where it pertains to the both the software and the hosting services provided by the Hosting Provider. Move to the top in the stack.
	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 Services	Hosting Provider Services is defined as: the Computer and Administration Services, Administration Services, and all other services provided by Hosting Provider which are ordered under and identified in the Ordering Document.
	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.
	Identity Management (IdM)	Identity Management (IdM) describes the management of individual identifiers, their authentication, authorization, and privileges within or across system and enterprise boundaries
	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 is defined as: 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 per the Agreement, 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.
	Interface	An interface is a point where two systems, subjects, organizations, etc., meet and interact.
	Interface Management Plan	An Interface Management Plan is a plan that will enumerate, document, and describe the necessary details concerning all the electronic interfaces that the Hosting Provider will create for the Customer. This may include non electronic interfaces if so deemed by the Customer.
	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.
	Monitoring Services	Monitoring Services are services or software that performs services that observe and check the progress or quality of the Customer Application and Customer Infrastructure over a period of time and keep under systematic review. Suggest we move it to the top and put into Definitions.
	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.
	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.
	Personally Identifiable Information (PII)	Personally Idenfitiable Information (PII) is defined as: information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
	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.
	Project Team	Project Team is defined as: a group of individuals working on a common objective or goal.
	Provisioning 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-oriented architecture (SOA)	Suggest adding the followingo Definitions. Service-oriented architecture (SOA) is a software design methodology based on structured collections of discrete software modules, known as services, that collectively provide the complete functionality of a large or complex software application.[1] Each service that makes up an SOA application is designed to provide a tightly defined set of functions. As a result, each service is built as a discrete piece of code.
	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.
	Shared Analytics Infrastructure	Shared Analytics Infrastructure Solutions consistitutes the shared software Solution engineered by the Hosting Provider to provide the Customer with the capability to analyze the data that has been gathered.
	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.
	Solution	Solution is defined as: the Environments, Applications, and software products running in the Hosting Provider Data Center(s) on behalf of the Customer
	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.
	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-Out Plan	"Transition-Out Plan" is a plan that articulates the steps and procedures that the Hosting Provider and the Customer will need to follow in order to successfully move the Customer's Infrastructure, Software, and Application to another Hosting Provider.
	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.
	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.
	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.

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 operated and maintained at the minimum Tier as set forth in the following pages per TIA 942 standards.		We are not Tier 3 in all areas, but have many tier 3 characteristics.	SOV completed a site visit and assessment of both CGI facilities and is agreement with finding on Sheet H1A TIA 942.
DC	1	2	DC.1.2	Data Center		Data center facilities will be located in the continental united states.			

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

The Hosting Provider shall deliver and maintain services from the Hosting Provider Data Center which meet or exceed the particular tier level of service for each line item, as defined on each in the Tier Rating column

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	T2		N/A
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	T2		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	T1			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			
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)	T2		#REF!
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 accessibie	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	If 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	T1	No seismic risk in Phx	#REF!
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	T1	No seismic risk in Phx	#REF!
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	T1	No seismic risk in Phx	#REF!
TIA	3	6	TIA.3.6	Data Center (Structural)	Structural		no	no	yes	yes	T1	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	N/A	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	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	N/A			#REF!
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	2 ATS's, Elec. Engineer contractor led shut down procedure	T1 ?	
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	on risk analysis as per NFPA 780 and insurance requirements.	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 Swtich PDU Automatic Transfer Switches	Main Transformer UPS Generator Feeder Circuit Breakers Automatic Static Transfer Swtich 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	Monitored 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	Generator	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 Integrated System	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	Not sure 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	N/A		#REF!
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	N/A		#REF!
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	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
H2	1	1	H2.1.1	Infrastructure	General	Hosting Provider will deliver infrastructure and related services from within its approved Data Centers.		
H2	1	2	H2.1.2	Infrastructure	General	Hosting Provider infrastructure will consist of dedicated servers, operating systems with shared local area network equipment, firewalls, routers, load balancers and any related equipment (shared or dedicated as required) and provided software		
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.		
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.		
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.		
H2	1	6	H2.1.6	Infrastructure	Acqusition and Provisioning	The Provisioning Release Plan will be used as the basis to install and configure the hardware, network, storage and software required for the environments.		
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		
H2	1	8	H2.1.8	Infrastructure	Acqusition and Provisioning	Hosting Provider will install Hosting Provider's Certified Configuration onto each provisioned Server		
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		
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)		
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		
H2	1	12	H2.1.12	Infrastructure	Acqusition and Provisioning	Hosting Provider will install and manage required Third Party Software		
H2	1	13	H2.1.13	Infrastructure	Acqusition and Provisioning	Hosting Provider will ensure implementation/deployment plans are aligned with the Provisioning Release Plan		
H2	1	14	H2.1.14	Infrastructure	Availability Management	Hosting Provider will provide Availability Management functions and data to the Customer.		
H2	1	15	H2.1.15	Infrastructure	Availability Management	Hosting Provider will utilize monitoring tools as part of Availability Management to identify actual or potential incidents affecting availability, and take action to prevent or minimize such impact. Customer must be notified when incidents are identified affecting Environment availability.		
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		
H2	1	17	H2.1.17	Infrastructure	Availability Management	Hosting Provider will maintain availability for all Environments, Applications, and software products running in the Hosting Provider Data Center(s) regardless of whether the Applications or software products were provided by and/or licensed to Hosting Provider.		
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, providing network characteristics sufficient to meet contractually defined Service Level Agreement(s).		
H2	1	19	H2.1.19	Infrastructure	General	Hosting Provider solution will utilize industry standard hardware(storage, servers, switches, firewalls, load balancers).		
H2	1	20	H2.1.20	Infrastructure	General	Hosting Provider will utilize industry standard virtualization technologies, and will deploy said virtualization technologies following the best practices of the selected virtualization vendor(s).		
H2	1	21	H2.1.21	Infrastructure	General	Hosting Provider will build Customers infrastructure utilizing physical and virtual separation and components		
H2	1	22	H2.1.22	Infrastructure	Design	Hosting Provider will assist Customer in preparing the detailed infrastructure requirements		
H2	1	23	H2.1.23	Infrastructure	Design			
H2	1	24	H2.1.24	Infrastructure	Design	Hosting Provider will utilize Customer requirements to design the Hosting Provider Environments and prepare a Provisioning Release Plan. Hosting Provider will then review the Provisioning Release Plan with the Customer.		
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		
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.)		
H2	1	27	H2.1.27	Infrastructure	Design	Hosting Provider will Collect and document, and publish all infrastructure/environments under Hosting Provider management		
H2	1	28	H2.1.28	Infrastructure	Environments	Hosting Provider will implement a high available Production Environment per Customers Production, Environment Diagram.		
H2	1	29	H2.1.29	Infrastructure	Environments	(PRODUCTION) Hosting Provider will implement a high available Production Environment per Customers Production Environment Diagram.		

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.		
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.		
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.		
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.		
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.		
H2	1	35	H2.1.35	Maintenance and Operations	Design	The Environments shall be scalable, enterprise-ready applications. The Environments shall support the deployment of other various types of distributed applications, and shall be constructed using best practices based on Service Oriented Architectures (SOA)		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Networking

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
H3	1	1	H3.1.1	Network	Bandwidth	Network bandwidth must be monitored and adjusted as program usage grows and changes.		
H3	1	2	H3.1.2	Network	Bandwidth	Hosting Provider shall implement minimum bandwidth requirements as a starting point for network sizing deployment.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
H3	1	13	H3.1.13	Network	DNS	Hosting Provider will configure the DNS to use the default Hosting Provider domain for application URLs. This URL is registered as a canonical name (CNAME) DNS record pointing to the Server address assigned to the Customer URL.		
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.		
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.}		
H3	1	16	H3.1.16	Network	General	Customer shall access the Hosting Provider Programs through a URL entered in a Web browser.		
H3	1	17	H3.1.17	Network	General	Hosting Provider will ensure that all network devices and links are properly sized and configured and are running optimally.		
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.		
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.		
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.		
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.		

H3	1	22	H3.1.22	Network	Hosting Provider Internal Service Network	The HPISN shall utilize redundant firewalls, intrusion detection systems (IDS), syslog and VPN technologies to secure the Environment. Default-deny rule sets shall be enforced by the firewall security policy, and an IDS shall monitor any potential violations of the predefined rules. In addition, the Hosting Provider shall be responsible for engaging a third party assessment vendor to perform periodic assessments of the Environment and deliver or review reports with the Customer		
H3	1	23	H3.1.23	Network	Hosting Provider Internal Service Network	The HPISN architecture shall assign static IP addresses to individual Hosting Provider personnel. As each user IP passes through the HPISN firewalls, Hosting Provider shall log and report the session activity to the Environment.		
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.		
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.		
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.		
H3	1	27	H3.1.27	Network	IDS	Hosting Provider shall employ IDS to provide continuous surveillance for intercepting and responding to security events as they are identified. Alerts shall be forwarded to Hosting Provider's IT security and the Hosting Provider Service Desk for review and response to potential threats.		
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.		
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.		
H3	1	30	H3.1.30	Network	IP Addresses	Hosting Provider will ensure that only routable IP addresses are presented to Hosting Provider		
H3	1	31	H3.1.31	Network	IP Addresses	Hosting Provider will specify IP addresses to route to Hosting Provider's Data Center(s)		
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.		
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.		
H3	1	34	H3.1.34	Network	IP addresses	Hosting Provider will perform the required translations for NAT if used.		
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.		
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		
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 Data Centers of less than 100ms from within the U.S.		
H3	1	38	H3.1.38	Network	Metrics	Hosting Provider will provide recommendations for network metrics		
H3	1	39	H3.1.39	Network	Monitoring	Hosting Provider will monitor network usage and resize as appropriate		
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 shall upgrade network links that exceed 80 percent of network capacity during peak usage.		
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.		
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		
H3	1	43	H3.1.43	Network	Performance	---		
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.		
H3	1	45	H3.1.45	Network	Routing	Hosting Provider will route traffic to Customer over the Transaction Link or Management Link, as applicable		
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.		

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.		
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.		
H3	1	49	H3.1.49	Network	SSL	The Hosting Provider shall procure and renew SSL certificates on Customer's behalf.		
H3	1	50	H3.1.50	Network	SSL	---		
H3	1	51	H3.1.51	Network	WAN	---		
H3	1	52	H3.1.52	Network	WAN	Hosting Provider shall establish a dedicated circuit between the Hosting Provider Data Center(s) and the Customer Data Center which shall only used for Hosting Provider Services.		
H3	1	53	H3.1.53	Network	WAN	---		
H3	1	54	H3.1.54	Network	WAN	---		
H3	1	55	H3.1.55	Network	WAN	---		
H3	1	56	H3.1.56	Network	WAN	---		
H3	1	57	H3.1.57	Network	WAN	---		
H3	1	58	H3.1.58	Network	WAN	---		
H3	1	59	H3.1.59	Network	WAN	---		
H3	1	60	H3.1.60	Network	WAN	---		
H3	1	61	H3.1.61	Network	WAN	---		
H3	1	62	H3.1.62	Network	WAN	---		
H3	1	63	H3.1.63	Network	WAN	---		
H3	1	64	H3.1.64	Network	WAN	---		
H3	1	65	H3.1.65	Network	WAN	---		
H3	1	66	H3.1.66	Network	WAN	---		
H3	1	67	H3.1.67	Network	General	Solutions will use TCP/IP as its networking protocol.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Backup Recovery

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
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.		
H4	1	2	H4.1.2	Backup Recovery	General	Backup Recovery Services will be in place for Production Environment and Non-Production Environments where applicable.		
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.		
H4	1	4	H4.1.4	Backup Recovery	General	In the event of a declaration Backup Recovery Services will be activated at the Disaster Recovery site.		
H4	1	5	H4.1.5	Backup Recovery	General	Full backups of Customers's Environments shall be taken weekly with incremental backups taken daily with data stored offsite with a required retention period of 7 years or EOC with supplier.		
H4	1	6	H4.1.6	Backup Recovery	General	Hosting Provider will perform and store production baseline backup of the database, application code tree, and archive logs, upon Customer's request.		
H4	1	7	H4.1.7	Backup Recovery	Overall availability	Backup solutions shall support 99.9% application availability.		
H4	1	8	H4.1.8	Backup Recovery	Recovery point objective	The recovery point objective (RPO) shall be 30 minutes		
H4	1	9	H4.1.9	Backup Recovery	Recovery time objective	The recovery time objective (RTO) shall be four (4) hours		
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.		
H4	1	11	H4.1.11	Backup Recovery	Offsite backup storage	One copy of the backup should store at off-site location daily.		
H4	1	12	H4.1.12	Backup Recovery	Availability during backup	Backups should be completed while the application is still active and supporting users.		
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.		
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.		
H4	1	15	H4.1.15	DR	DR testing	The DR facility will be tested annually for full recovery within a 4 hour recovery timeframe.		
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.		
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.	Iron Mountain is 28.5 miles from the CGI Phoenix Data Center	

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Capacity and Performance Management

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
H5	1	1	H5.1.1	Capacity / Performance Management		---		
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.		
H5	1	3	H5.1.3	Capacity / Performance Management		Hosting Provider will collect performance and capacity metrics		
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		
H5	1	5	H5.1.5	Capacity / Performance Management		Hosting Provider will conduct Capacity Management periodically as part of the Periodic Maintenance Plan		
H5	1	6	H5.1.6	Capacity / Performance Management		Hosting Provider will periodically review storage requirements and alert Customer as capacity limits are approached		
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		
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		
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		
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.)		
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		
H5	1	12	H5.1.12	Capacity / Performance Management		Hosting Provider will ensure batch workload is distributed across all available and appropriate system resources		
H5	1	13	H5.1.13	Capacity / Performance Management	Load Balancing	Hardware and Network should support load balancing technologies for high availability and maintenance		
H5	1	14	H5.1.14	Capacity / Performance Management	Continuous scalability	Server workloads should scale on-demand without shutting down the application		
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		
H5	1	16	H5.1.16	Capacity / Performance Management	Seasonable load scalability	Server capacity should support month end and year end processing capacity		
H5	1	17	H5.1.17	Capacity / Performance Management	Peak Concurrent Internal Users	System should support 400 concurrent internal users at peak time (6:00am - 6:00pm EST).		
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).		
H5	1	19	H5.1.19	Capacity / Performance Management	Peak Concurrent External Users	System should support 400 concurrent external users at peak time (6:00am - 6:00pm EST).		
H5	1	20	H5.1.20	Capacity / Performance Management	Off-peak Concurrent External Users	System should support 400 concurrent internal users during Off-Peak hours (6:00pm - 6:00am EST).		
H5	1	21	H5.1.21	Capacity / Performance Management	Server CPU utilization	The server(s) CPU utilization is not to exceed 85%		
H5	1	22	H5.1.22	Capacity / Performance Management	Server memory utilization	The server(s) memory utilization is not to exceed 90%		
H5	1	23	H5.1.23	Capacity / Performance Management	Server storage utilization	The server(s) disk space utilization is not to exceed 80%		
H5	1	24	H5.1.24	Capacity / Performance Management	LAN collision rate	The Local Area Network (LAN) collision rate is not to exceed 20%		

H5	1	25	H5.1.25	Capacity / Performance Management	WAN utilization	The Wide Area Network (WAN) utilization is not to exceed 80%		
H5	1	26	H5.1.26	Capacity / Performance Management	Storage growth	Storage systems shall have the capability if necessary to expand up to 20% in size per year		
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		
H5	1	28	H5.1.28	Capacity / Performance Management	Switch standard clustered databases	Clustering of database servers and application should connect thru private network.		
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.		
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.		
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.		
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.		
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.		
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.		
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).		
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		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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. (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.		
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.		
H5	1	47	H5.1.47	Capacity / Performance Management	A4.4	Solutions shall return a parameter-based report within 20 seconds or less.(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. (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).		
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		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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).		
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.		
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.		
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.		
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.		
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		
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.		
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.		
H5	1	68	H5.1.68	Capacity / Performance Management	UI Response Time	UI level transaction should complete in 5 seconds (on average)		
H5	1	69	H5.1.69	Capacity / Performance Management	Query Response Time	Query thru UI layer should show results in 15 seconds (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		
H5	1	71	H5.1.71	Capacity / Performance Management	non-functional	Hosting Provider shall develop, maintain, and enforce a Capacity Plan.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Configuration Management

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
H6	1	1	H6.1.1	Configuration Management		Hosting Provider shall implement and maintain Configuration Management documentation and processes.		
H6	1	2	H6.1.2	Configuration Management		Hosting Provider will maintain an Architecture Document to represent the current configuration of the Environment		
H6	1	3	H6.1.3	Configuration Management		Hosting Provider will account for all IT assets and configurations within the Environment		
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		
H6	1	5	H6.1.5	Configuration Management		Hosting Provider will maintain accurate documentation on configurations to support other service management processes		
H6	1	6	H6.1.6	Configuration Management		Hosting Provider will maintain configuration records of changes to Third Party Software		
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.		
H6	1	8	H6.1.8	Configuration Management		---		
H6	1	9	H6.1.9	Configuration Management		Supplier shall develop a technical infrastructure document which describes all of the hardware, system software and tools necessary for each proposed deployment environment. Due date is 9/1/13 unless changed to some other date mutually agreed upon. Hosting provider is responsible to communicate to the Customer in order to successfully complete.		
H6	1	10	H6.1.10	Configuration Management		Supplier shall develop an environment configuration manual that describes the environment installation and configuration necessary deployent environment. Due date is 9/1/13 unless changed to some other date mutually agreed upon. Hosting provider is responsible to communicate to the Customer in order to successfully complete.		
H6	1	11	H6.1.11	Configuration Management		---		
H6	1	12	H6.1.12	Configuration Management		Supplier shall provide the State with readable source code and object (executable) code, documentation for all functionality developed by Supplier, 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. Due date is 9/1/13 unless changed to some other date mutually agreed upon. Hosting provider is responsible to communicate to the Customer in order to successfully complete.		
H6	1	13	H6.1.13	Configuration Management		Supplier shall provide a data dictionary and data model for the State.		
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)		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Release Management

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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.		
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.		
H7	1	3	H7.1.3	Release Management		Hosting Provider will perform maintenance on Infrastructure as specified by the SLA		
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")		
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.		
H7	1	6	H7.1.6	Release Management		Infrastructure Components may include but are not limited to Servers, network devices, and storage.		
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		
H7	1	8	H7.1.8	Release Management		Hosting Provider will use commercially reasonable efforts to coordinate the timing of Release-related maintenance activities		
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		
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. Supplier shall provide updated documentation when upgrades to software or equipment occurs through the life of the contract or project.		
H7	1	11	H7.1.11	Release Management		Upon successful completion of the pre-production testing, Supplier shall, in coordination with the Customer, create a Production Release Plan. The Project Release Plan shall consist of an updated Pre-Production Release notification (this is a notification/warning) 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		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Monitoring Management

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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		
H8	1	2	H8.1.2	Monitoring		Hosting Provider will identify event threshold violations for proactive response		
H8	1	3	H8.1.3	Monitoring		Hosting Provider will facilitate configuration of monitoring events		
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		
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		
H8	1	6	H8.1.6	Monitoring		Hosting Provider will report Outages and Service Interruptions when identified		
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		
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.		
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.		
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		
H8	1	11	H8.1.11	Monitoring	transaction monitoring and logging	Solutions shall allow for different roles for Users including Operators, Administrators, Managers etc		
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.		
H8	1	13	H8.1.13	Monitoring	transaction monitoring and logging	---		
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.		
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.		
H8	1	16	H8.1.16	Monitoring	transaction monitoring and logging	Solutions shall detect intrusion attempts by unauthorized system users.		
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.		
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		
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.		
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.		
H8	1	21	H8.1.21			Hosting Provider shall utilize a network-based monitoring approach to detect attacks on open firewalls ports.		
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.		

H8	1	23	H8.1.23			Network instrusion alerts are forwarded to Hosting Providers IT security and Service Desk immediately for review and response.		
H8	1	24	H8.1.24			Hosting provider shall employ a separate extranet for hosting servers separating them from its internal corporate network.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Service Continuity Management

Base	Level	Sub	Req ID New	Requirement Description	Notes	Evidence
H9	1	1	H9.1.1	Hosting Provider will provide Service Continuity Management for the Production Environment following a declared Disaster.		
H9	1	2	H9.1.2	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.		
H9	1	3	H9.1.3	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.		
H9	1	4	H9.1.4	Hosting Provider will conduct regular system backups of the Environment(s) following the frequency and retention outlined by Customer.		
H9	1	5	H9.1.5	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.		
H9	1	6	H9.1.6	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.		
H9	1	7	H9.1.7	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.		
H9	1	8	H9.1.8	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.		
H9	1	9	H9.1.9	Solutions (Application Services) shall be restored in less than 4 hours (RTO), and only experience the loss of the 30 minutes (RPO) of transactions.		
H9	1	10	H9.1.10	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.		
H9	1	11	H9.1.11	Solutions shall include a disaster recovery plan and provide contingency plans to Customer for application services managed by Hosting Provider.		
H9	1	12	H9.1.12	Production Environment shall have a Disaster Recovery plan which includes Business Continuity components for the Exchange M&O as provided by the supplier		
H9	1	13	H9.1.13	Solutions will maintain and effectively implement plans for emergency response, backup operations and post disaster recovery		

H9	1	14	H9.1.14	Disaster recovery requirements relative to the physical solution components and planning for recovery from operational failures are the responsibility of Supplier . Supplier 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.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Refreshes and Lifecycle

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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).		
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.		
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.		
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").		
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.		
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.		
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.		
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.		
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.		
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.		
H10	1	11	H10.1.11	Refreshes and Lifecycle		Hosting provider will develop with Customer a Refresh Schedule to perform the Refreshes identified.		
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.		
H10	1	13	H10.1.13	Refreshes and Lifecycle		Hosting provider will perform Refreshes in accordance with standard Hosting Provider procedures and guidelines.		
H10	1	14	H10.1.14	Refreshes and Lifecycle		Hosting provider will perform Refreshes based on a submitted and approved change request from Customer		
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.		
H10	1	16	H10.1.16	Refreshes and Lifecycle		Hosting provider shall work with one contact at Customer for coordination of refreshes		
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.		
H7	1	18	H7.1.18	Release Manager		Database Data exports can contain all data from Customer's Production database(s).		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Maintenance and Operations

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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		
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		
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		
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.		
H11	1	5	H11.1.5	Maintenance and Operations	non-functional	Supplier shall describe the production support and transition approach and methodology used for solutions.		
H11	1	6	H11.1.6	Maintenance and Operations	non-functional	Supplier shall establish an automated maintenance routine that shall at a minimum: - backup the user IDs and password data - identify expired IDs and related data		
H11	1	7	H11.1.7	Maintenance and Operations	non-functional	Upon completion of any maintenance call, Supplier 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.		
H11	1	8	H11.1.8	Maintenance and Operations	non-functional	Supplier 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.		
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.		
H11	1	10	H11.1.10	Maintenance and Operations	non-functional	Supplier 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.		
H11	1	11	H11.1.11	Maintenance and Operations	non-functional	Supplier shall provide documentation that describes the procedures for Solution administrators to add, update or remove user IDs and passwords.		
H11	1	12	H11.1.12	Maintenance and Operations	non-functional	Supplier 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		
H11	1	13	H11.1.13	Maintenance and Operations	non-functional	Supplier shall provide the responsible entity with help desk scripts and decision trees for tier 1 and 2 help desk support.		
H11	1	14	H11.1.14	Maintenance and Operations	non-functional	Supplier 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.		
H11	1	15	H11.1.15	Maintenance and Operations	non-functional	Supplier shall provide instructions and training for responsible agency support staff that may need to access and support the solution remotely.		

H11	1	16	H11.1.16	Maintenance and Operations	non-functional	Supplier 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 Supplier intends to support the solution and transition that support over to the entity responsible for on-going production operations and support.		
H11	1	17	H11.1.17	Maintenance and Operations	non-functional	Supplier shall agree to continue normal operations activities until completion of Transition-Out Plan activities.		
H11	1	18	H11.1.18	Maintenance and Operations	non-functional	Supplier shall, at a minimum, provide routine solution upgrades and fixes to the solution components at no additional cost. In addition, Supplier 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, subcontractors, manufacturers, and other third parties.		
H11	1	19	H11.1.19	Maintenance and Operations	non-functional	Supplier shall provide the State with a list of personnel, contact information, and their area of expertise of who shall be performing solution production support.		
H11	1	20	H11.1.20	Maintenance and Operations	non-functional	Supplier shall repair any corrupted data that is associated with a problem in the solution.		
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. Hosting Provider shall provide the State with a copy of the schedule at least 30 days in advance of the scheduled maintenance date for approval.		
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.		
H11	1	23	H11.1.23	Maintenance and Operations	non-functional	Supplier 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).		
H11	1	24	H11.1.24	Maintenance and Operations	non-functional	Supplier shall develop an automated process for purging production solution files when necessary.		
H11	1	25	H11.1.25	Maintenance and Operations	non-functional	The Solution as defined in the Definition section shall be compatible with the State's Enterprise Management Components. The solution as defined in the Definition section shall protect and monitor at the network and application level. Application is defined in the Definition section.		
H11	1	26	H11.1.26	Maintenance and Operations	non-functional	Application logs and error messages shall be monitored by the Hosting Provider.		
H11	1	27	H11.1.27	Maintenance and Operations	non-functional	Web-based solutions shall permit analysis of web logs		
H11	1	28	H11.1.28	Maintenance and Operations	non-functional			
H11	1	29	H11.1.29	Maintenance and Operations	non-functional	Solutions shall have critical security patches applied within 24 hours		
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		
H11	1	31	H11.1.31	Maintenance and Operations	non-functional	Solutions will include a supported release of all software.		
H11	1	32	H11.1.32	Maintenance and Operations	non-functional	Solutions will support automated patch deployment.		
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.		
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.		

H11	1	35	H11.1.35	Maintenance and Operations	non-functional	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). Hosting Provoder will deliver by 9/1/2013 unless another date is mutually agreed upon. 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 * Defect/Issue management".		
H11	1	36	H11.1.36	Maintenance and Operations	non-functional	Solutions shall provide data archiving capabilities based on State defined criteria.		
H11	1	37	H11.1.37	Maintenance and Operations	non-functional	All Solution communications shall be protected by at least 128-bit encryption.		
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.		
H11	1	39	H11.1.39	Maintenance and Operations	non-functional	Solutions shall provide admin tools and maintenance routines to change access rights quickly.		
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.		
H11	1	41	H11.1.41	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to create and manage user accounts.		
H11	1	42	H11.1.42	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign status and permissions to user accounts.		
H11	1	43	H11.1.43	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to create and manage user roles.		
H11	1	44	H11.1.44	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to create user groups to manage workflow.		
H11	1	45	H11.1.45	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign users to particular local offices.		
H11	1	46	H11.1.46	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign users to particular user groups / units.		
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.		

H11	1	48	H11.1.48	Maintenance and Operations	non-functional	Solutions shall allow Solution administrators to assign users to particular supervisors.		
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.		
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.		
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.		
H11	1	52	H11.1.52	Maintenance and Operations	non-functional	Solutions shall provide logging, reporting for accessing errors and exceptions.		
H11	1	53	H11.1.53	Maintenance and Operations	non-functional	Solutions shall monitor and provide reports on any unauthorized access.		
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.		
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.		
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.		
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.		
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)		
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		
H11	1	60	H11.1.60	Maintenance and Operations	non-functional	Supplier shall describe the implementation approach and methodology used for projects.		
H11	1	61	H11.1.61	Maintenance and Operations	non-functional	Supplier shall develop a Software Configuration Management Plan.		
H11	1	62	H11.1.62	Maintenance and Operations	non-functional	Supplier 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.		
H11	1	63	H11.1.63	Maintenance and Operations	non-functional	Supplier must use an industry standard software configuration management tool.		
H11	1	64	H11.1.64	Maintenance and Operations	non-functional			
H11	1	65	H11.1.65	Maintenance and Operations	non-functional	Supplier 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.		
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.		
H11	1	67	H11.1.67	Maintenance and Operations	non-functional	Supplier 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.		
H11	1	68	H11.1.68	Maintenance and Operations	non-functional	Supplier shall assist the State with testing and release preparation in the pre-production environment.		
H11	1	69	H11.1.69	Maintenance and Operations	non-functional	Supplier must produce and execute an On-Site Implementation Support Plan.		

H11	1	70	H11.1.70	Maintenance and Operations	non-functional	Supplier 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 Supplier in the plan's construction, with particular attention to high complexity components of the existing the State systems as well as the proposed solution.		
H11	1	71	H11.1.71	Maintenance and Operations	non-functional	Supplier must provide staff at the proposed number, ratios and duration for on-site support (as identified in previously submitted implementation approach and plan).		
H11	1	72	H11.1.72	Maintenance and Operations	non-functional	Supplier must assess the pre-implementation readiness of each part of the organization and shall document the status in a pre-implementation readiness assessment. Supplier shall conduct an implementation readiness review ten days prior to cutover at each part of the organization.		
H11	1	73	H11.1.73	Maintenance and Operations	non-functional	---		
H11	1	74	H11.1.74	Maintenance and Operations	non-functional	---		
H11	1	75	H11.1.75	Maintenance and Operations	non-functional	---		
H11	1	76	H11.1.76	Maintenance and Operations	non-functional	Supplier shall produce a lessons learned document after conducting the Solution component pilots and provide recommendations for changes to the implementation process.		
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.		
H11	1	78	H11.1.78	Maintenance and Operations	non-functional	Supplier shall describe the interface management approach and methodology used for the solution.		
H11	1	79	H11.1.79	Maintenance and Operations	non-functional	Supplier 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		
H11	1	80	H11.1.80	Maintenance and Operations	non-functional	Supplier shall validate that each interface is working correctly. Supplier will repair all interface-related problems caused by Hosting Provider-developed interfaces.		
H11	1	81	H11.1.81	Maintenance and Operations	non-functional	Supplier shall assist the State in identifying root causes for all solutions' interface related problems.		
H11	1	82	H11.1.82	Maintenance and Operations	non-functional	Solutions will leverage permitted hosting environments to support their respective technology needs		
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		
H11	1	84	H11.1.84	Maintenance and Operations	non-functional	Solutions will ensure that environments are synchronized to ensure adequate pre-production testing		
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		
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.		

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		
H11	1	88	H11.1.88	Maintenance and Operations	non-functional	Application and technology components shall support session replication to support transparent fail over.		
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		
H11	1	90	H11.1.90	Maintenance and Operations	non-functional	Solutions requiring a JEE server should utilize Oracle WebLogic Server		
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		
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		
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.		
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		
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		
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		
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		
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		
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.		
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.		
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.		
H11	1	102	H11.1.102	Maintenance and Operations	Solution	The solution shall provide a standardized mechanism for Conflict Management and data integrity.		
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.		
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		
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.		
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.)		
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.		
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.		
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.		
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.		
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.		

H11	1	112	H11.1.112	Maintenance and Operations	Contractor	The contractor shall maintain reliable business operations in accordance with the agreed upon SLA.		
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.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Hosting Governance

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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.		
H12	1	2	H12.1.2	Hosting Governance	Governance	Governance Services will 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.		
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.		
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.		
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.		
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.		
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.		
H12	1	8	H12.1.8	Hosting Governance	Account Plan Management	---		
H12	1	9	H12.1.9	Hosting Governance	Account Plan Management	---		
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.		
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.		
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.		
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.		
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.		
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.		
H12	1	16	H12.1.16	Hosting Governance	Availability Management	Hosting Provider will provide an Availablility Plan to Customer detailing Production Environment availability. It deliverable by 9/1/2013 or at a mutually agreed upon time.		
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.		
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.		
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.		
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.		
H12	1	21	H12.1.21	Hosting Governance	Capacity Management	Hosting Provider will work with Customer to integrate required changes into the Production Environment.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		

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.		
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.		
H12	1	31	H12.1.31	Hosting Governance	Service Management	Hosting Provider will Produce and articulate a Service Management Plan		
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.		
H12	1	33	H12.1.33	Hosting Governance	Service Management	Hosting Provider will provide Service Plans to Customer detailing the schedule of tactical events.		
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.		
H12	1	35	H12.1.35	Hosting Governance	Service Management	Hosting Provider will track and monitor execution of scheduled events.		
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.		
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.		
H12	1	38	H12.1.38	Hosting Governance	Service Management	Hosting Provider will monitor and measure the operational performance of the Hosting Provider Services.		
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.		
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.		
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.		
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").		
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.		
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.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Service Level Agreement SLA

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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.		
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.		
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%		
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%		
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.		
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.		
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		
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 docuemnted 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.		
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.		
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.		
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.		
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.		
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 in the Continental/Contiguous United States (CONUS) at Hosting Provider'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.		
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		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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		

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:			
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.			
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			
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			
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 failiure, 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.			
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.			
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			
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			
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.			
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.			
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.			
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.			
H13	1	35	H13.1.35		Hosting, SLA, Stabilization Period (required)	Each Stabilization Period will be seven 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.			
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.			
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			
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			
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.			
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			
H13	1	41	H13.1.41			The Contractor shall be held accountable to issue resolution standards as defined by the agreed upon SLA.			TC-62
H13	1	42	H13.1.42			Solutions shall provide Service Level Agreement (SLA) monitoring and reporting capabilities.			Q4.3
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.			TC-70
H13	1	44	H13.1.44			The contractor shall provide routine maintenance periods as defined by the agreed upon SLA.			TC-69

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Security Summary

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
S1	1	1	S1.1.1	SOV		Hosting Provider will follow State of Vermont Secuirty Standards. http://dii.vermont.gov/Policy_Central		
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.		
S1	1	3	S1.1.3			Hosting Provider and Solutions shall comply with Federal Security standards outlined in S3 Federal Security work sheets.		
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 moderate impact security category under FIPS 199.		
S1	1	5	S1.1.5	DoD Standards		Solutions shall comply with DoD Directive 8552.01		
S1	1	6	S1.1.6	FISMA Standards		Solutions shall comply with Federal Information Security Management Act (FISMA) of 2002		
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.		
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.		
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).		
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.		
		11	S1.1.11	HIPAA Standards		Hosting Provider infrastructure and Hosting Provider Software shall comply with HIPAA standards.		
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.		
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		
S1	1	14	S1.1.14	ACA		Solutions shall comply with the Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations		
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.		
S1	1	16	S1.1.16			Hosting Provider and Solutions shall comply with IRS 1075 standards outlined see Exhibit D.		
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). See Exhibit D.		
S1	1	18	S1.1.18	PCI DSS		Hosting Provider and Solutions shall comply with PCI/DSS standards. Solutions using credit/debit or other electronic funds transfer cards shall be compliant with Payment Card Industry (PCI) security standards. See Exhibit D.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Security General

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
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.		
S2A	1	2	S2A.1.2	Security General		Hosting Provider provides database activity logging, monitoring, and reporting of the production database instances of the Hosting Provider ePHI Environments while protecting audit trails 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.		
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.		
S2A	1	4	S2A.1.4	Security General		---		
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.		
S2A	1	6	S2A.1.6	Security General		Database data shall be encrypted at the file system layer		
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.		
S2A	1	8	S2A.1.8	Security General		Hosting Provider will conduct annual reviews of Vermont's Hosting Provider Hosting Provider network router configurations.		
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.		
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.		
S2A	1	11	S2A.1.11	Security General		---		
S2A	1	12	S2A.1.12	Security General		---		
S2A	1	13	S2A.1.13	Security General		---		
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.		
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		
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.		
S2A	1	17	S2A.1.17	Security General		Hosting Provider shall conduct quarterly scans of Vermont's externally accessible web service on the Production Environment, and provide reports on the scans, including the severity of the vulnerabilities and remediation recommendations.		

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.		
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		
S2A	1	20	S2A.1.20	Security General		Hosting Provider shall provide Operating System management to protect against dictionary and brute force attacks.		
S2A	1	21	S2A.1.21	Security General		Access to ePHI Servers shall be restricted to those employees who have completed HIPAA training.		
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.		
S2A	1	23	S2A.1.23	Security General		Network router configurations shall be reviewed annually		
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.		
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.		
S2A	1	26	S2A.1.26	Security General		Strong authentication shall be employed in all deployment environments		
S2A	1	27	S2A.1.27	Security General		Self-registered users of applications shall have identities verified per NIST SP800-63		
S2A	1	28	S2A.1.28	Security General		HBE-related Solutions shall proof identities based on requirements set forth by CMS		
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		
S2A	1	30	S2A.1.30	Security General		Solutions shall have the ability to manage atomic-to-composite role mappings		
S2A	1	31	S2A.1.31	Security General		Solutions shall have the ability to provide better performance for applications that use fine-grained policies (bulk security)		
S2A	1	32	S2A.1.32	Security General		Solutions shall support Federal Identity, Credential, and Access Management ("FICAM") Roadmap and Implementation Guidelines		
S2A	1	33	S2A.1.33	Security General		Solutions shall support Protection of PII data		
S2A	1	34	S2A.1.34	Security General		Solutions shall integrate with federal security services for identity proofing and multi-factor authentication		
S2A	1	35	S2A.1.35	Security General		module design and implementation must take into account security standards and controls as documented by NIST		
S2A	1	36	S2A.1.36	Security General		Project participants and other individuals shall not transmit or store any Personally Identifiable Information (PII) using storage publically available, over the Internet or any wireless communication device, unless: 1) the PII is "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 Customer.		
S2A	1	37	S2A.1.37	Security General		All Solutions shall adhere to applicable state and federal laws regarding Privacy and Security, as well as the policies and procedures set forth in the Agreement.		
S2A	1	38	S2A.1.38	Security General		Solutions will provide a mechanism to securely authorize staff and customers to access the authorized functionality.		
S2A	1	39	S2A.1.39	Security General		Solutions will define the level of access that will be granted to each particular role.		
S2A	1	40	S2A.1.40	Security General		Solutions will utilize encryption algorithms and implementations, in compliance with National Institute of Standards and Technology.		

S2A	1	41	S2A.1.41	Security General		The Solutions will have a potential fraud detection function.		
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.		
S2A	1	43	S2A.1.43	Security General		Solutions will define the data elements displayed to users based on privilege set/ role		
S2A	1	44	S2A.1.44	Security General		User privileges shall be periodically audited		
S2A	1	45	S2A.1.45	Security General		Solutions will identify and define access roles for cross-organizational information systems		
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		
S2A	1	47	S2A.1.47	Security General		Solutions will log all unsuccessful login attempts.		
S2A	1	48	S2A.1.48	Security General		Application and technology components shall integrate and rely on the centralized IdM infrastructure		
S2A	1	49	S2A.1.49	Security General		The Hosting Provider shall ensure that the Solution and Service Center complies with all applicable State of Vermont Information Security Policies.		
S2A	1	50	S2A.1.50	Security General		The Solutions will enforce a single system identify for each unique user involved with the Exchange.		
S2A	1	51	S2A.1.51	Security General		The Solution will be able to establish family or household linkages between individual accounts.		
S2A	1	52	S2A.1.52	Security General		The Solution shall provide intrusion detection and prevention services.		
S2A	1	53	S2A.1.53	Security General		The Solution shall provide Certificate Authority for secure server side transactions.		
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.		
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.).		
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.		
S2A	1	57	S2A.1.57	Security General		The Solution shall support issue and manage public key certificates for secure transactions.		
S2A	1	58	S2A.1.58	Security General		The Solution shall support the ability to verify and validate identity via public key certificates for secure transactions.		
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		
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.		
S2A	1	61	S2A.1.61	Security General		The Solution shall support penetration testing from external vendors.		
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.		
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.		
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.		

S2A	1	65	S2A.1.65	Security General		The Solution shall manage user profiles including defining access to data types and security credentials.		
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.		
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.		
S2A	1	68	S2A.1.68	Security General		The Solution shall restrict access to user, provider, or organizational data to authorized users.		
S2A	1	69	S2A.1.69	Security General		The Solution shall ensure non-repudiation as part of digital signature verification to prevent data from being altered, deleted or damaged during exchange.		
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.		
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.		
S2A	1	72	S2A.1.72	Security General		The Solution shall implement and support two-factor authentication (i.e. two kinds of evidence).		
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.		
S2A	1	74	S2A.1.74	Security General		The Solution shall provide the ability to implement security for transport and messaging via web services.		
S2A	1	75	S2A.1.75	Security General		The Solution shall track all access so that an audit report of an individual's information can be provided to the individual if requested.		
S2A	1	76	S2A.1.76	Security General		The Solution shall provide ability to the Customer to disable all types of user accounts.		
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.		
S2A	1	78	S2A.1.78	Security General		---		
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.		
S2A	1	80	S2A.1.80	Security General		The contractor shall ensure that the Exchange Solution system documentation is protected from unauthorized access.		
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.		
S2A	1	82	S2A.1.82	Security General	CHIP Compliand	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.		
S2A	1	83	S2A.1.83	Security General	FIMA Compliani	Modules must also comply with the Federal Information Security Management Act of 2002 (FISMA).		
S2A	1	84	S2A.1.84	Security General	HIPAA Compliar	Modules must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security and privacy requirements, including standards soon to be promulgated		
S2A	1	85	S2A.1.85	Security General	Existing Identity	Healthcare-related Solutions shall utilize or comply with existing data field, validation methods, and policies for identity management.		
S2A	1	86	S2A.1.86	Security General		Solutions shall support identification, authentication, and authorization management.		
S2A	1	87	S2A.1.87	Security General		Public facing Solutions shall provide a mechanism for customers to register for an account.		
S2A	1	88	S2A.1.88	Security General		Public facing Solutions shall allow customers to manage their user account.		
S2A	1	89	S2A.1.89	Security General		Solutions shall provide a mechanism to control user access.		
S2A	1	90	S2A.1.90	Security General		Solutions shall provide a mechanism to authenticate users.		

S2A	1	91	S2A.1.91	Security General		Solutions and security-related technology components shall provide a mechanism to administer password policies.		
S2A	1	92	S2A.1.92	Security General		Solutions shall support administration password policies.		
S2A	1	93	S2A.1.93	Security General		Solutions will secure data to maintain customer privacy.		
S2A	1	94	S2A.1.94	Security General		The Solution will gather, store and maintain, as confidential, personal income data to establish eligibility for coverage (i.e., Income tax returns, Social Security number).		
S2A	1	95	S2A.1.95	Security General		Suggest changing system to Solution. See next. The Solution 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.		
S2A	1	96	S2A.1.96	Security General		Solutions will comply with relevant security laws, policies, processes and standards.		
S2A	1	97	S2A.1.97	Security General		Solutions will ensure that data is secured and only accessible to authorized individuals		
S2A	1	98	S2A.1.98	Security General		Solutions will safeguard computer systems, peripherals and assets.		
S2A	1	99	S2A.1.99	Security General		Solutions will protect customer information from unauthorized disclosure.		
S2A	1	100	S2A.1.100	Security General	Directory Attribute Naming	Directory attributes shall conform to VT naming standards and core set of attributes		
S2A	1	101	S2A.1.101	Security General	Virtual Directory Services	Identity Management systems shall be implemented using a 'virtual directory' model in order to abstract directory sources and improve maintainability.		
S2A	1	102	S2A.1.102	Security General	Directory Separation	Separate directories shall be used for employees and external users. Additional directory segmentation TBD		
S2A	1	103	S2A.1.103	Security General	Directory LDAP Accessibility	Directories shall be accessible via the LDAP protocol		
S2A	1	104	S2A.1.104	Security General	SSO	Solutions shall utilize SSO components for authentication and authorization		
S2A	1	105	S2A.1.105	Security General		The Solution shall have role based access control at the data field level		
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)		
S2A	1	107	S2A.1.107	Security General	CMS	Hosting Provider shall 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).		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Security General B

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
S2B	1	1	S2B.1.1	Hosting, General Security Services		Security assessments shall be performed prior to releasing solutions into production		
S2B	1	2	S2B.1.2	Hosting, General Security Services,		---		
S2B	1	3	S2B.1.3	Hosting, General Security Services,		---		
S2B	1	4	S2B.1.4	Hosting, General Security Services,		Failure of a Hosting Provider 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.		
S2B	1	5	S2B.1.5	Hosting, General Security Services,		---		
S2B	1	6	S2B.1.6	Hosting, General Security Services,		---		
S2B	1	7	S2B.1.7	Hosting, General Security Services,		---		
S2B	1	8	S2B.1.8	Hosting, General Security Services,		---		
S2B	1	9	S2B.1.9	Hosting, General Security Services,		---		
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.		
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.		
S2B	1	12	S2B.1.12	Hosting, General Security Services, Access Control		Least Privilege shall be employed for all solutions.		
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.		
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.		
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.		
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.		
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, on an annual basis at minimum. At the conclusion of each test, the commander must submit a gap analysis report to incident response management along with recommendations for corrective actions.		
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.		
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 Customer or destroyed in accordance with the Hosting Provider Information Protection Policy.		
S2B	1	20	S2B.1.20	Hosting, General Security Services, Audits		---		
S2B	1	21	S2B.1.21	Hosting, General Security Services, Backup and Recovery Procedure		---		
S2B	1	22	S2B.1.22	Hosting, General Security Services, Backup and Recovery Procedure		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.		
S2B	1	23	S2B.1.23	Hosting, General Security Services, Backup and Recovery Procedure		---		
S2B	1	24	S2B.1.24	Hosting, General Security Services, Backup and Recovery Procedure		---		
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		
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		
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 Customer. Customer 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.		
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).		
S2B	1	29	S2B.1.29	Hosting, General Security Services, Backup and Recovery Procedure		Administrative access to key management system is role-based.		

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).		
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.		
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 isolcated from other customers' components.		
S2B	1	33	S2B.1.33	Hosting, General Security Services, Breach Policy		Access controls to network, system, database, and application layers shall be multi-tieried and accessible on a default-deny basis		
S2B	1	34	S2B.1.34	Hosting, General Security Services, Breach Policy		Hosting Provider shall share relevant Breach, Security, and Enforcement policies with the Customer		
S2B	1	35	S2B.1.35	Hosting, General Security Services, Chain of Custody		Hosting Provider shall utilize a single point of contact ("commander") for security incidents. The commander shall assume the command 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.		
S2B	1	36	S2B.1.36	Hosting, General Security Services, Clear Desk and Clear Screen		---		
S2B	1	37	S2B.1.37	Hosting, General Security Services, Clear Desk and Clear Screen	Screen Lock	---		
S2B	1	38	S2B.1.38	Hosting, General Security Services, Cloud Services Risk Management		Hosting Provider shall maintain a Security Organization Policy describing and clarifying the roles and responsibilities of various teams and individuals involved in information security at Hosting Provider.		
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.		
S2B	1	40	S2B.1.40	Hosting, General Security Services, Compliance with Laws and the European Union Data Privacy Directive		---		
S2B	1	41	S2B.1.41	Hosting, General Security Services, Compliance with Laws and the European Union Data Privacy Directive		---		
S2B	1	42	S2B.1.42	Hosting, General Security Services, Compliance with Laws and the European Union Data Privacy Directive		---		
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 shall subscribe to an agreement under which any Hosting Provider subsidiary handling Customer data adopts safeguards consistent with those between the Hosting Provider and the Customer for Hosting Provider Services.		
S2B	1	44	S2B.1.44	Hosting, General Security Services, Confidentiality		---		
S2B	1	45	S2B.1.45	Hosting, General Security Services, Confidentiality Agreements		---		
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.		
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 sufficent 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.		
S2B	1	48	S2B.1.48	Hosting, General Security Services, Data Center Physical Controls		---		
S2B	1	49	S2B.1.49	Hosting, General Security Services, Data Center Physical Controls		---		
S2B	1	50	S2B.1.50	Hosting, General Security Services, Data Center Physical Controls		---		
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.		
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.		

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.		
S2B	1	54	S2B.1.54	Hosting, General Security Services, Data Center Physical Controls		Visitors to the Hosting Provider Data Center(s) shall be banned from possessing weapons, recording devices and alcohol while on Data Center premises.		
S2B	1	55	S2B.1.55	Hosting, General Security Services, Data Center Physical Controls		Visitor badges for the Hosting Provider Data Center(s) shall be inventoried on a nightly basis. Any badge identified as missing shall be immediately deactivated.		
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.		
S2B	1	57	S2B.1.57	Hosting, General Security Services, Data Center Physical Controls		---		
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 Provider's employees, subcontractors, and authorized visitors.		
S2B	1	59	S2B.1.59	Hosting, General Security Services, Data Center Physical Controls		Hosting Provider Data Center employees, subcontractors, and authorized visitors shall be issued identification cards that must be worn while on the premises.		
S2B	1	60	S2B.1.60	Hosting, General Security Services, Data Center Physical Controls		Visitors to Hosting Provider Data Center(s) 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.		
S2B	1	61	S2B.1.61	Hosting, General Security Services, Data Center Physical Controls		Hosting Provider's Security monitors the possession of keys/access cards and the ability to access the Hosting Provider Data Center(s). Employees leaving employment must return keys/cards immediately.		
S2B	1	62	S2B.1.62	Hosting, General Security Services, Data Center Physical Controls		After-hours access to Hosting Provider Data Center(s) shall be monitored and controlled by Hosting Provider Security.		
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.		
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.		
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.		
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.		
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.		
S2B	1	68	S2B.1.68	Hosting, General Security Services, Environment/Application Security		---		
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 Hosting Provider Data Center(s).		
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.)		
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.		
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.		
S2B	1	73	S2B.1.73	Hosting, General Security Services, Exchange of Information		Server disk drives shall be sanitized by degaussing.		
S2B	1	74	S2B.1.74	Hosting, General Security Services, Exchange of Information		Hosting Provider Data Center(s) shall maintain designated areas to store defective or expired media until sanitized and/or transported to third party for secure destruction.		
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.		
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.		
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.		
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.		

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:			
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.			
S2B	1	81	S2B.1.81	Hosting, General Security Services, Health Insurance Portability and Accountability Act (HIPAA) Compliance		---			
S2B	1	82	S2B.1.82	Hosting, General Security Services, Health Insurance Portability and Accountability Act (HIPAA) Compliance		---			
S2B	1	83	S2B.1.83	Hosting, General Security Services, Hosting Provider's Business Continuity Management Program		In the event of a security incident, the Hosting Provider shall be responsible for collecting and retaining evidence related to the incident.			
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.			
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 a security incident.			
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.			
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.			
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.			
S2B	1	89	S2B.1.89	Hosting, General Security Services, Information Disposal		Hosting Provider shall not disclose Customer data except in accordance with the Statement of Work, subsequent written instructions by Customer, or as required by law.			
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.			
S2B	1	91	S2B.1.91	Hosting, General Security Services, Information Labeling and Handling		---			
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.			
S2B	1	93	S2B.1.93	Hosting, General Security Services, Information Security Incident Response – Reporting Breaches		---			
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.			
S2B	1	95	S2B.1.95	Hosting, General Security Services, Information Security Incident Response – Reporting Breaches		---			
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			
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 Information Security Incident Response Team (ISIRT) 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.			
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.			

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 templates pre-defined by the Hosting Provider.		
S2B	1	100	S2B.1.100	Hosting, General Security Services, Information Systems Acquisition, Development, and Maintenance		---		
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.		
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.		
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:		
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		
S2B	1	105	S2B.1.105	Hosting, General Security Services, ISO 27001 Certification for the Information Security System		---		
S2B	1	106	S2B.1.106	Hosting, General Security Services, ISO 27002 Certificate of Conformance		---		
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.		
S2B	1	108	S2B.1.108	Hosting, General Security Services, ISO 27002 Certificate of Conformance		---		
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 internal and external, global communications, Ensure continuity of key functions in a work around manner until normalcy is restored, and Ensure recovery of computing/technology infrastructure and services.		
S2B	1	110	S2B.1.110	Hosting, General Security Services, Legally Required Disclosures		---		
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.		
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.		
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.		
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.		
S2B	1	115	S2B.1.115	Hosting, General Security Services, Logging		---		
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).		
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.		
S2B	1	118	S2B.1.118	Hosting, General Security Services, Media Handling and Disposal		Customer data shall not be stored on any type of removable drive or medium unless the information is encrypted.		
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.		
S2B	1	120	S2B.1.120	Hosting, General Security Services, Media Handling and Disposal		---		
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.		
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.		
S2B	1	123	S2B.1.123	Hosting, General Security Services, Mobile Computing and Teleworking		---		

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.		
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.		
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		
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		
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.		
S2B	1	129	S2B.1.129	Hosting, General Security Services, Network Connection Control		---		
S2B	1	130	S2B.1.130	Hosting, General Security Services, Network Routing Control		---		
S2B	1	131	S2B.1.131	Hosting, General Security Services, Network Security Management		Restoration of data is tested annually.		
S2B	1	132	S2B.1.132	Hosting, General Security Services, Organizational Security		---		
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.		
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.		
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.		
S2B	1	136	S2B.1.136	Hosting, General Security Services, Payment Card Industry Data Security Standard		---		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
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.		
S2B	1	145	S2B.1.145	Hosting, General Security Services, Protection Against Malicious Code		Hosting Provider personnel shall be required to install approved full disk encryption software on their laptops, which uses a strong encryption algorithm.		
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.		
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.		
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.		

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.		
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.		
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.		
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.		
S2B	1	153	S2B.1.153	Hosting, General Security Services, Secure Login Procedures		---		
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.		
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		
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		
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.		
S2B	1	158	S2B.1.158	Hosting, General Security Services, Security Awareness Education and Training		---		
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.		
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		
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.		
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.		
S2B	1	163	S2B.1.163	Hosting, General Security Services, Security Services		Hosting Provider will limit direct administrative access to Vermont's SaU 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.		
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.		
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.		
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.		
S2B	1	167	S2B.1.167	Hosting, General Security Services, Sensitive System Isolation		Database auditing will be enabled.		
S2B	1	168	S2B.1.168	Hosting, General Security Services, Sensitive System Isolation		Production Environments shall be isolated from Non-Production Environments.		
S2B	1	169	S2B.1.169	Hosting, General Security Services, Sensitive System Isolation		All deployment environments shall be isolated from one another.		
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).		
S2B	1	171	S2B.1.171	Hosting, General Security Services, Session Time Out		Servers shall enable default log file settings for auditing critical events		
S2B	1	172	S2B.1.172	Hosting, General Security Services, SSAE and ISAE Reports and Other Audits		---		
S2B	1	173	S2B.1.173	Hosting, General Security Services, SSAE and ISAE Reports and Other Audits		---		

S2B	1	174	S2B.1.174	Hosting, General Security Services, SSAE and ISAE Reports and Other Audits		---		
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.		
S2B	1	176	S2B.1.176	Hosting, General Security Services, System Acceptance		Capacity planning and management shall occur throughout the hosting life cycle.		
S2B	1	177	S2B.1.177	Hosting, General Security Services, System Acceptance		---		
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.		
S2B	1	179	S2B.1.179	Hosting, General Security Services, System Acceptance		---		
S2B	1	180	S2B.1.180	Hosting, General Security Services, System Passwords	Passowrd Confidentiality	Passwords shall be treated as confidential information.		
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.		
S2B	1	182	S2B.1.182	Hosting, General Security Services, System Planning		---		
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.		
S2B	1	184	S2B.1.184	Hosting, General Security Services, Third Party Service Delivery		---		
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.		
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 the Customer's or Hosting Provider's access provisioning process.		
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 Customer 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.		
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		
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?		
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.		
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.		
S2B	1	192	S2B.1.192	Hosting, General Security Services, User Password Management	Password Strength Audit	Passwords shall be peridocially audited to ensure they comply with the Password Strength requirements		
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.		
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.		
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.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Security General

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
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.		
S3	1	2	S3.1.2	Federal Security	General	Hosting Provider will provide dedicated physical and virtual infrastructure to Vermont		
S3	1	3	S3.1.3	Federal Security	General	---		
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.		
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.		
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.		
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.		
S3	1	8	S3.1.8	Federal Security	General	Hosting Provider will provide Maintenance of the Vermont Federal Environment Infrastructure.		
S3	1	9	S3.1.9	Federal Security	Certification and Accreditation	Hosting Provider will limit data in the Federal Environment to Unclassified data.		
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).		
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.		
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.		
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.		
S3	1	14	S3.1.14	Federal Security	Data Sensitivity Classification	---		
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.		
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.		
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.		
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 moderate impact security category under FIPS 199.		
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.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

NIST 800 Series

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
AC	00		AC-00	Access Control	Access Control Group	Hosting Provider can meet all Access Control measures in the Access Control Group		
AC	01		AC-01	Access Control	AC-01	Access Control Policy and Procedures		
AC	02		AC-02	Access Control	AC-02	Account Management		
AC	03		AC-03	Access Control	AC-03	Access Enforcement		
AC	04		AC-04	Access Control	AC-04	Information Flow Enforcement		
AC	05		AC-05	Access Control	AC-05	Separation of Duties		
AC	06		AC-06	Access Control	AC-06	Least Privilege		
AC	07		AC-07	Access Control	AC-07	Unsuccessful Login Attempts		
AC	08		AC-08	Access Control	AC-08	System Use Notification		
AC	09		AC-09	Access Control	AC-09	Previous Logon (Access) Notification		
AC	10		AC-10	Access Control	AC-10	Concurrent Session Control		
AC	11		AC-11	Access Control	AC-11	Session Lock		
AC	12		AC-12	Access Control	AC-12	Session Termination (Withdrawn)		
AC	13		AC-13	Access Control	AC-13	Supervision and Review—Access Control (Withdrawn)		
AC	14		AC-14	Access Control	AC-14	Permitted Actions without Identification or Authentication		
AC	15		AC-15	Access Control	AC-15	Automated Marking (Withdrawn)		
AC	16		AC-16	Access Control	AC-16	Security Attributes		
AC	17		AC-17	Access Control	AC-17	Remote Access		
AC	18		AC-18	Access Control	AC-18	Wireless Access		
AC	19		AC-19	Access Control	AC-19	Access Control for Mobile Devices		
AC	20		AC-20	Access Control	AC-20	Use of External Information Systems		
AC	21		AC-21	Access Control	AC-21	User-Based Collaboration and Information Sharing		
AC	22		AC-22	Access Control	AC-22	Publicly Accessible Content		
AT	00		AT-00	Awareness and Training	Awareness and Training Control Group	Hosting Provider can meet all Awareness and Training measures in the Awareness and Training Control Group		
AT	01		AT-01	Awareness and Training	AT-01	Security Awareness and Training Policy and Procedures		
AT	02		AT-02	Awareness and Training	AT-02	Security Awareness		
AT	03		AT-03	Awareness and Training	AT-03	Security Training		
AT	04		AT-04	Awareness and Training	AT-04	Security Training Records		
AT	05		AT-05	Awareness and Training	AT-05	Contacts with Security Groups and Associations		
AU	00		AU-00	Audit and Accountability	Audit and Accountability Control Group	Hosting Provider can meet all Audit and Accountability measures in the Audit and Accountability Control Group		
AU	01		AU-01	Audit and Accountability	AU-01	Audit and Accountability Policy and Procedures		
AU	02		AU-02	Audit and Accountability	AU-02	Auditable Events		
AU	03		AU-03	Audit and Accountability	AU-03	Content of Audit Records		
AU	04		AU-04	Audit and Accountability	AU-04	Audit Storage Capacity		
AU	05		AU-05	Audit and Accountability	AU-05	Response to Audit Processing Failures		
AU	06		AU-06	Audit and Accountability	AU-06	Audit Review, Analysis, and Reporting		
AU	07		AU-07	Audit and Accountability	AU-07	Audit Reduction and Report Generation		
AU	08		AU-08	Audit and Accountability	AU-08	Time Stamps		
AU	09		AU-09	Audit and Accountability	AU-09	Protection of Audit Information		
AU	10		AU-10	Audit and Accountability	AU-10	Non-repudiation		
AU	11		AU-11	Audit and Accountability	AU-11	Audit Record Retention		
AU	12		AU-12	Audit and Accountability	AU-12	Audit Generation		
AU	13		AU-13	Audit and Accountability	AU-13	Monitoring for Information Disclosure		
AU	14		AU-14	Audit and Accountability	AU-14	Session Audit		
CA	00		CA-00	Security Assessment and Authorization	Security Assessment and Authorization Control Group	Hosting Provider can meet all Security Assessment and Authorization measures in the Security Assessment and Authorization Control Group		
CA	01		CA-01	Security Assessment and Authorization	CA-01	Security Assessment and Authorization Policies and Procedures		
CA	02		CA-02	Security Assessment and Authorization	CA-02	Security Assessments		
CA	03		CA-03	Security Assessment and Authorization	CA-03	Information System Connections		

CA	04		CA-04	Security Assessment and Authorization	CA-04	Security Certification (Withdrawn)		
CA	05		CA-05	Security Assessment and Authorization	CA-05	Plan of Action and Milestones		
CA	06		CA-06	Security Assessment and Authorization	CA-06	Security Authorization		
CA	07		CA-07	Security Assessment and Authorization	CA-07	Continuous Monitoring		
CM	00		CM-00	Configuration Management	Configuration Management Control Group	Hosting Provider can meet all Configuration Management measures in the Configuration Management Control Group		
CM	01		CM-01	Configuration Management	CM-01	Configuration Management Policy and Procedures		
CM	02		CM-02	Configuration Management	CM-02	Baseline Configuration		
CM	03		CM-03	Configuration Management	CM-03	Configuration Change Control		
CM	04		CM-04	Configuration Management	CM-04	Security Impact Analysis		
CM	05		CM-05	Configuration Management	CM-05	Access Restrictions for Change		
CM	06		CM-06	Configuration Management	CM-06	Configuration Settings		
CM	07		CM-07	Configuration Management	CM-07	Least Functionality		
CM	08		CM-08	Configuration Management	CM-08	Information System Component Inventory		
CM	09		CM-09	Configuration Management	CM-09	Configuration Management Plan		
CP	00		CP-00	Contingency Planning	Contingency Planning Control Group	Hosting Provider can meet all Contingency Planning measures in the Contingency Planning Control Group		
CP	01		CP-01	Contingency Planning	CP-01	Contingency Planning Policy and Procedures		
CP	02		CP-02	Contingency Planning	CP-02	Contingency Plan		
CP	03		CP-03	Contingency Planning	CP-03	Contingency Training		
CP	04		CP-04	Contingency Planning	CP-04	Contingency Plan Testing and Exercises		
CP	05		CP-05	Contingency Planning	CP-05	Contingency Plan Update (Withdrawn)		
CP	06		CP-06	Contingency Planning	CP-06	Alternate Storage Site		
CP	07		CP-07	Contingency Planning	CP-07	Alternate Processing Site		
CP	08		CP-08	Contingency Planning	CP-08	Telecommunications Services		
CP	09		CP-09	Contingency Planning	CP-09	Information System Backup		
CP	10		CP-10	Contingency Planning	CP-10	Information System Recovery and Reconstitution		
IA	00		IA-00	Identification and Authentication	Identification and Authentication Control Group	Hosting Provider can meet all Identification and Authentication measures in the Identification and Authentication Control Group		
IA	01		IA-01	Identification and Authentication	IA-01	Identification and Authentication Policy and Procedures		
IA	02		IA-02	Identification and Authentication	IA-02	Identification and Authentication (Organizational Users)		
IA	03		IA-03	Identification and Authentication	IA-03	Device Identification and Authentication		
IA	04		IA-04	Identification and Authentication	IA-04	Identifier Management		
IA	05		IA-05	Identification and Authentication	IA-05	Authenticator Management		
IA	06		IA-06	Identification and Authentication	IA-06	Authenticator Feedback		
IA	07		IA-07	Identification and Authentication	IA-07	Cryptographic Module Authentication		
IA	08		IA-08	Identification and Authentication	IA-08	Identification and Authentication (Non-Organizational Users)		
IR	00		IR-00	Incident Response	Incident Response Control Group	Hosting Provider can meet all Incident Response measures in the Incident Response Control Group		
IR	01		IR-01	Incident Response	IR-01	Incident Response Policy and Procedures		
IR	02		IR-02	Incident Response	IR-02	Incident Response Training		
IR	03		IR-03	Incident Response	IR-03	Incident Response Testing and Exercises		
IR	04		IR-04	Incident Response	IR-04	Incident Handling		
IR	05		IR-05	Incident Response	IR-05	Incident Monitoring		
IR	06		IR-06	Incident Response	IR-06	Incident Reporting		
IR	07		IR-07	Incident Response	IR-07	Incident Response Assistance		
IR	08		IR-08	Incident Response	IR-08	Incident Response Plan		

MA	00		MA-00	Maintenance	Maintenance Control Group	Hosting Provider can meet all Maintenance measures in the Maintenance Control Group		
MA	01		MA-01	Maintenance	MA-01	System Maintenance Policy and Procedures		
MA	02		MA-02	Maintenance	MA-02	Controlled Maintenance		
MA	03		MA-03	Maintenance	MA-03	Maintenance Tools		
MA	04		MA-04	Maintenance	MA-04	Non-Local Maintenance		
MA	05		MA-05	Maintenance	MA-05	Maintenance Personnel		
MA	06		MA-06	Maintenance	MA-06	Timely Maintenance		
MP	00		MP-00	Media Protection	Media Protection Control Group	Hosting Provider can meet all Media Protection measures in the Media Protection Control Group		
MP	01		MP-01	Media Protection	MP-01	Media Protection Policy and Procedures		
MP	02		MP-02	Media Protection	MP-02	Media Access		
MP	03		MP-03	Media Protection	MP-03	Media Marking		
MP	04		MP-04	Media Protection	MP-04	Media Storage		
MP	05		MP-05	Media Protection	MP-05	Media Transport		
MP	06		MP-06	Media Protection	MP-06	Media Sanitization		
PE	00		PE-00	Physical and Environmental Protection	Physical and Environmental Protection Control Group	Hosting Provider can meet all Physical and Environmental Protection measures in the Physical and Environmental Protection Control Group		
PE	01		PE-01	Physical and Environmental Protection	PE-01	Physical and Environmental Protection Policy and Procedures		
PE	02		PE-02	Physical and Environmental Protection	PE-02	Physical Access Authorizations		
PE	03		PE-03	Physical and Environmental Protection	PE-03	Physical Access Control		
PE	04		PE-04	Physical and Environmental Protection	PE-04	Access Control for Transmission Medium		
PE	05		PE-05	Physical and Environmental Protection	PE-05	Access Control for Output Devices		
PE	06		PE-06	Physical and Environmental Protection	PE-06	Monitoring Physical Access		
PE	07		PE-07	Physical and Environmental Protection	PE-07	Visitor Control		
PE	08		PE-08	Physical and Environmental Protection	PE-08	Access Records		
PE	09		PE-09	Physical and Environmental Protection	PE-09	Power Equipment and Power Cabling		
PE	10		PE-10	Physical and Environmental Protection	PE-10	Emergency Shutoff		
PE	11		PE-11	Physical and Environmental Protection	PE-11	Emergency Power		
PE	12		PE-12	Physical and Environmental Protection	PE-12	Emergency Lighting		
PE	13		PE-13	Physical and Environmental Protection	PE-13	Fire Protection		
PE	14		PE-14	Physical and Environmental Protection	PE-14	Temperature and Humidity Controls		
PE	15		PE-15	Physical and Environmental Protection	PE-15	Water Damage Protection		
PE	16		PE-16	Physical and Environmental Protection	PE-16	Delivery and Removal		
PE	17		PE-17	Physical and Environmental Protection	PE-17	Alternate Work Site		
PE	18		PE-18	Physical and Environmental Protection	PE-18	Location of Information System Components		
PE	19		PE-19	Physical and Environmental Protection	PE-19	Information Leakage		
PL	00		PL-00	Planning	Planning Control Group	Hosting Provider can meet all Planning measures in the Planning Control Group		
PL	01		PL-01	Planning	PL-01	Security Planning Policy and Procedures		
PL	02		PL-02	Planning	PL-02	System Security Plan		
PL	03		PL-03	Planning	PL-03	System Security Plan Update (Withdrawn)		
PL	04		PL-04	Planning	PL-04	Rules of Behavior		

PL	05		PL-05	Planning	PL-05	Privacy Impact Assessment		
PL	06		PL-06	Planning	PL-06	Security-Related Activity Planning		
PS	00		PS-00	Personnel Security	Personnel Security Control Group	Hosting Provider can meet all Personnel Security measures in the Personnel Security Control Group		
PS	01		PS-01	Personnel Security	PS-01	Personnel Security Policy and Procedures		
PS	02		PS-02	Personnel Security	PS-02	Position Categorization		
PS	03		PS-03	Personnel Security	PS-03	Personnel Screening		
PS	04		PS-04	Personnel Security	PS-04	Personnel Termination		
PS	05		PS-05	Personnel Security	PS-05	Personnel Transfer		
PS	06		PS-06	Personnel Security	PS-06	Access Agreements		
PS	07		PS-07	Personnel Security	PS-07	Third-Party Personnel Security		
PS	08		PS-08	Personnel Security	PS-08	Personnel Sanctions		
RA	00		RA-00	Risk Assessment	Risk Assessment Control Group	Hosting Provider can meet all Risk Assessment measures in the Risk Assessment Control Group		
RA	01		RA-01	Risk Assessment	RA-01	Risk Assessment Policy and Procedures		
RA	02		RA-02	Risk Assessment	RA-02	Security Categorization		
RA	03		RA-03	Risk Assessment	RA-03	Risk Assessment		
RA	04		RA-04	Risk Assessment	RA-04	Risk Assessment Update (Withdrawn)		
RA	05		RA-05	Risk Assessment	RA-05	Vulnerability Scanning		
SA	00		SA-00	System and Services Acquisition	System and Services Acquisition Control Group	Hosting Provider can meet all System and Services Acquisition measures in the System and Services Acquisition Control Group		
SA	01		SA-01	System and Services Acquisition	SA-01	System and Services Acquisition Policy and Procedures		
SA	02		SA-02	System and Services Acquisition	SA-02	Allocation of Resources		
SA	03		SA-03	System and Services Acquisition	SA-03	Life Cycle Support		
SA	04		SA-04	System and Services Acquisition	SA-04	Acquisitions		
SA	05		SA-05	System and Services Acquisition	SA-05	Information System Documentation		
SA	06		SA-06	System and Services Acquisition	SA-06	Software Usage Restrictions		
SA	07		SA-07	System and Services Acquisition	SA-07	User-Installed Software		
SA	08		SA-08	System and Services Acquisition	SA-08	Security Engineering Principles		
SA	09		SA-09	System and Services Acquisition	SA-09	External Information System Services		
SA	10		SA-10	System and Services Acquisition	SA-10	Developer Configuration Management		
SA	11		SA-11	System and Services Acquisition	SA-11	Developer Security Testing		
SA	12		SA-12	System and Services Acquisition	SA-12	Supply Chain Protection		
SA	13		SA-13	System and Services Acquisition	SA-13	Trustworthiness		
SA	14		SA-14	System and Services Acquisition	SA-14	Critical Information System Components		
SC	00		SC-00	System and Communications Protection	System and Communications Protection Control Group	Hosting Provider can meet all System and Communications Protection measures in the System and Communications Protection Control Group		
SC	01		SC-01	System and Communications Protection	SC-01	System and Communications Protection Policy and Procedures		
SC	02		SC-02	System and Communications Protection	SC-02	Application Partitioning		
SC	03		SC-03	System and Communications Protection	SC-03	Security Function Isolation		
SC	04		SC-04	System and Communications Protection	SC-04	Information in Shared Resources		
SC	05		SC-05	System and Communications Protection	SC-05	Denial of Service Protection		

SC	06		SC-06	System and Communications Protection	SC-06	Resource Priority		
SC	07		SC-07	System and Communications Protection	SC-07	Boundary Protection		
SC	08		SC-08	System and Communications Protection	SC-08	Transmission Integrity		
SC	09		SC-09	System and Communications Protection	SC-09	Transmission Confidentiality		
SC	10		SC-10	System and Communications Protection	SC-10	Network Disconnect		
SC	11		SC-11	System and Communications Protection	SC-11	Trusted Path		
SC	12		SC-12	System and Communications Protection	SC-12	Cryptographic Key Establishment and Management		
SC	13		SC-13	System and Communications Protection	SC-13	Use of Cryptography		
SC	14		SC-14	System and Communications Protection	SC-14	Public Access Protections		
SC	15		SC-15	System and Communications Protection	SC-15	Collaborative Computing Devices		
SC	16		SC-16	System and Communications Protection	SC-16	Transmission of Security Attributes		
SC	17		SC-17	System and Communications Protection	SC-17	Public Key Infrastructure Certificates		
SC	18		SC-18	System and Communications Protection	SC-18	Mobile Code		
SC	19		SC-19	System and Communications Protection	SC-19	Voice Over Internet Protocol		
SC	20		SC-20	System and Communications Protection	SC-20	Secure Name /Address Resolution Service (Authoritative Source)		
SC	21		SC-21	System and Communications Protection	SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)		
SC	22		SC-22	System and Communications Protection	SC-22	Architecture and Provisioning for Name/Address Resolution Service		
SC	23		SC-23	System and Communications Protection	SC-23	Session Authenticity		
SC	24		SC-24	System and Communications Protection	SC-24	Fail in Known State		
SC	25		SC-25	System and Communications Protection	SC-25	Thin Nodes		
SC	26		SC-26	System and Communications Protection	SC-26	Honeypots		
SC	27		SC-27	System and Communications Protection	SC-27	Operating System-Independent Applications		
SC	28		SC-28	System and Communications Protection	SC-28	Protection of Information at Rest		
SC	29		SC-29	System and Communications Protection	SC-29	Heterogeneity		
SC	30		SC-30	System and Communications Protection	SC-30	Virtualization Techniques		
SC	31		SC-31	System and Communications Protection	SC-31	Covert Channel Analysis		
SC	32		SC-32	System and Communications Protection	SC-32	Information System Partitioning		
SC	33		SC-33	System and Communications Protection	SC-33	Transmission Preparation Integrity		
SC	34		SC-34	System and Communications Protection	SC-34	Non-Modifiable Executable Programs		
SI	00		SI-00	System and Information Integrity	System and Information Integrity Control Group	Hosting Provider can meet all System and Information Integrity measures in the System and Information Integrity Control Group		

SI	01		SI-01	System and Information Integrity	SI-01	System and Information Integrity Policy and Procedures		
SI	02		SI-02	System and Information Integrity	SI-02	Flaw Remediation		
SI	03		SI-03	System and Information Integrity	SI-03	Malicious Code Protection		
SI	04		SI-04	System and Information Integrity	SI-04	Information System Monitoring		
SI	05		SI-05	System and Information Integrity	SI-05	Security Alerts, Advisories, and Directives		
SI	06		SI-06	System and Information Integrity	SI-06	Security Functionality Verification		
SI	07		SI-07	System and Information Integrity	SI-07	Software and Information Integrity		
SI	08		SI-08	System and Information Integrity	SI-08	Spam Protection		
SI	09		SI-09	System and Information Integrity	SI-09	Information Input Restrictions		
SI	10		SI-10	System and Information Integrity	SI-10	Information Input Validation		
SI	11		SI-11	System and Information Integrity	SI-11	Error Handling		
SI	12		SI-12	System and Information Integrity	SI-12	Information Output Handling and Retention		
SI	13		SI-13	System and Information Integrity	SI-13	Predictable Failure Prevention		
PM	00		PM-00	Program Management	Program Management Control Group	Hosting Provider can meet all Program Management measures in the Program Management Control Group		
PM	01		PM-01	Program Management	PM-01	Information Security Program Plan		
PM	02		PM-02	Program Management	PM-02	Senior Information Security Officer		
PM	03		PM-03	Program Management	PM-03	Information Security Resources		
PM	04		PM-04	Program Management	PM-04	Plan of Action and Milestones Process		
PM	05		PM-05	Program Management	PM-05	Information System Inventory		
PM	06		PM-06	Program Management	PM-06	Information Security Measures of Performance		
PM	07		PM-07	Program Management	PM-07	Enterprise Architecture		
PM	08		PM-08	Program Management	PM-08	Critical Infrastructure Plan		
PM	09		PM-09	Program Management	PM-09	Risk Management Strategy		
PM	10		PM-10	Program Management	PM-10	Security Authorization Process		
PM	11		PM-11	Program Management	PM-11	Mission/Business Process Definition		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

NIST 800 Series

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
AC			AC-01.01-00	AC-01 ACCESS CONTROL POLICY AND PROCEDURES	AC-01.01-00	See Exhibit F		
			AC-01.01-01	AC-01 ACCESS CONTROL POLICY AND PROCEDURES	AC-01.01-01	See Exhibit F		
			AC-01.01-02	AC-01 ACCESS CONTROL POLICY AND PROCEDURES	AC-01.01-02	See Exhibit F		
				AC-01 ACCESS CONTROL POLICY AND PROCEDURES	Supplemental Guidance	See Exhibit F		
			AC-02.01-00	AC-02 ACCOUNT MANAGEMENT	AC-02.01-00	See Exhibit F		
			AC-02.01-01	AC-02 ACCOUNT MANAGEMENT	AC-02.01-01	See Exhibit F		
			AC-02.01-02	AC-02 ACCOUNT MANAGEMENT	AC-02.01-02	See Exhibit F		
			AC-02.01-03	AC-02 ACCOUNT MANAGEMENT	AC-02.01-03	See Exhibit F		
			AC-02.01-04	AC-02 ACCOUNT MANAGEMENT	AC-02.01-04	See Exhibit F		
			AC-02.01-05	AC-02 ACCOUNT MANAGEMENT	AC-02.01-05	See Exhibit F		
			AC-02.01-06	AC-02 ACCOUNT MANAGEMENT	AC-02.01-06	See Exhibit F		
			AC-02.01-07	AC-02 ACCOUNT MANAGEMENT	AC-02.01-07	See Exhibit F		
			AC-02.01-08	AC-02 ACCOUNT MANAGEMENT	AC-02.01-08	See Exhibit F		
			AC-02.01-09	AC-02 ACCOUNT MANAGEMENT	AC-02.01-09	See Exhibit F		
			AC-02.01-10	AC-02 ACCOUNT MANAGEMENT	AC-02.01-10	See Exhibit F		
				AC-02 ACCOUNT MANAGEMENT	Supplemental Guidance	See Exhibit F		
			AC-02(1).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(1).01-00	See Exhibit F		
			AC-02(2).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(2).01-00	See Exhibit F		
			AC-02(3).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(3).01-00	See Exhibit F		
			AC-02(4).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(4).01-00	See Exhibit F		
			AC-02(5).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-00	See Exhibit F		
			AC-02(5).01-01	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-01	See Exhibit F		
			AC-02(5).01-02	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-02	See Exhibit F		
			AC-02(5).01-03	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-03	See Exhibit F		
			AC-02(5).01-04	AC-02 CONTROL ENHANCEMENTS	AC-02(5).01-04	See Exhibit F		
			AC-02(6).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(6).01-00	See Exhibit F		
				AC-02 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-02(7).01-00	AC-02 CONTROL ENHANCEMENTS	AC-02(7).01-00	See Exhibit F		
			AC-02(7).01-01	AC-02 CONTROL ENHANCEMENTS	AC-02(7).01-01	See Exhibit F		
			AC-02(7).01-02	AC-02 CONTROL ENHANCEMENTS	AC-02(7).01-02	See Exhibit F		
			AC-03.01-00	AC-03 ACCESS ENFORCEMENT	AC-03.01-00	See Exhibit F		

				AC-03 CONTROL ENHANCEMENTS	Supplemental Guidance	See Exhibit F		
			AC-03(1).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(1).01-00	See Exhibit F		
			AC-03(2).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(2).01-00	See Exhibit F		
				AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-03(3).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(3).01-00	See Exhibit F		
			AC-03(3).01-01	AC-03 CONTROL ENHANCEMENTS	AC-03(3).01-01	See Exhibit F		
			AC-03(3).01-02	AC-03 CONTROL ENHANCEMENTS	AC-03(3).01-02	See Exhibit F		
				AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
				AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-03(4).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-00	See Exhibit F		
			AC-03(4).01-01	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-01	See Exhibit F		
			AC-03(4).01-02	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-02	See Exhibit F		
			AC-03(4).01-03	AC-03 CONTROL ENHANCEMENTS	AC-03(4).01-03	See Exhibit F		
			AC-03(5).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(5).01-00	See Exhibit F		
				AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-03(6).01-00	AC-03 CONTROL ENHANCEMENTS	AC-03(6).01-00	See Exhibit F		
				AC-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04.01-00	AC-4 INFORMATION FLOW ENFORCEMENT	AC-04.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			AC-04(1).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(1).01-00	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(2).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(2).01-00	See Exhibit F		
			AC-04(3).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(3).01-00	See Exhibit F		
			AC-04(4).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(4).01-00	See Exhibit F		
			AC-04(5).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(5).01-00	See Exhibit F		
			AC-04(6).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(6).01-00	See Exhibit F		
			AC-04(7).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(7).01-00	See Exhibit F		
			AC-04(8).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(8).01-00	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(9).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(9).01-00	See Exhibit F		
			AC-04(10).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(10).01-00	See Exhibit F		
			AC-04(11).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(11).01-00	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(12).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(12).01-00	See Exhibit F		

				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(13).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(13).01-00	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(14).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(14).01-00	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(15).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(15).01-00	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(16).01-00	Control Enhancements:	AC-04(16).01-00	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-04(17).01-00	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-00	See Exhibit F		
			AC-04(17).01-01	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-01	See Exhibit F		
			AC-04(17).01-02	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-02	See Exhibit F		
			AC-04(17).01-03	AC-04 CONTROL ENHANCEMENTS	AC-04(17).01-03	See Exhibit F		
				AC-04 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-05.01-00	AC-05 SEPARATION OF DUTIES	AC-05.01-00	See Exhibit F		
			AC-05.01-01	AC-05 SEPARATION OF DUTIES	AC-05.01-01	See Exhibit F		
			AC-05.01-02	AC-05 SEPARATION OF DUTIES	AC-05.01-02	See Exhibit F		
			AC-05.01-03	AC-05 SEPARATION OF DUTIES	AC-05.01-03	See Exhibit F		
				AC-05 SEPARATION OF DUTIES	Supplemental Guidance	See Exhibit F		
			AC-06.01-00	AC-06 LEAST PRIVILEGE	AC-06.01-00	See Exhibit F		
				AC-06 LEAST PRIVILEGE	Supplemental Guidance	See Exhibit F		
			AC-06(1).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(1).01-00	See Exhibit F		
				AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-06(2).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(2).01-00	See Exhibit F		
				AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-06(3).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(3).01-00	See Exhibit F		
			AC-06(4).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(4).01-00	See Exhibit F		
				AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-06(5).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(5).01-00	See Exhibit F		
				AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-06(6).01-00	AC-06 CONTROL ENHANCEMENTS	AC-06(6).01-00	See Exhibit F		
				AC-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-07.01-00	AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	AC-07.01-00	See Exhibit F		
			AC-07.01-01	AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	AC-07.01-01	See Exhibit F		

			AC-07.01-02	AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	AC-07.01-02	See Exhibit F		
				AC-07 UNSUCCESSFUL LOGIN ATTEMPTS	Supplemental Guidance	See Exhibit F		
			AC-07(1).01-00	AC-07 CONTROL ENHANCEMENTS	AC-07(1).01-00	See Exhibit F		
			AC-07(2).01-00	AC-07 CONTROL ENHANCEMENTS	AC-07(2).01-00	See Exhibit F		
				AC-07 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-08.01-00	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-00	See Exhibit F		
			AC-08.01-01	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-01	See Exhibit F		
			AC-08.01-02	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-02	See Exhibit F		
			AC-08.01-03	AC-08 SYSTEM USE NOTIFICATION	AC-08.01-03	See Exhibit F		
				AC-08 SYSTEM USE NOTIFICATION	Supplemental Guidance	See Exhibit F		
			AC-09.01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09.01-00	See Exhibit F		
				AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	Supplemental Guidance	See Exhibit F		
			AC-09(1).01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09(1).01-00	See Exhibit F		
			AC-09(2).01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09(2).01-00	See Exhibit F		
			AC-09(3).01-00	AC-09 PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-09(3).01-00	See Exhibit F		
			AC-10.01-00	AC-10 CONCURRENT SESSION CONTROL	AC-10.01-00	See Exhibit F		
				AC-10 CONCURRENT SESSION CONTROL	Supplemental Guidance	See Exhibit F		
			AC-11.01-00	AC-11 SESSION LOCK	AC-11.01-00	See Exhibit F		
			AC-11.01-01	AC-11 SESSION LOCK	AC-11.01-01	See Exhibit F		
			AC-11.01-02	AC-11 SESSION LOCK	AC-11.01-02	See Exhibit F		
				AC-11 SESSION LOCK	Supplemental Guidance	See Exhibit F		
			AC-11(1).01-00	AC-11 CONTROL ENHANCEMENTS	AC-11(1).01-00	See Exhibit F		
			AC-12.01-00	AC-12 SESSION TERMINATION	AC-12.01-00	See Exhibit F		
			AC-13.01-00	AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL	AC-13.01-00	See Exhibit F		
			AC-14.01-00	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR	AC-14.01-00	See Exhibit F		
			AC-14.01-01	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR	AC-14.01-01	See Exhibit F		
			AC-14.01-02	AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR	AC-14.01-02	See Exhibit F		
				AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR	Supplemental Guidance	See Exhibit F		
			AC-14(1).01-00	AC-14 CONTROL ENHANCEMENTS	AC-14(1).01-00	See Exhibit F		
			AC-15.01-00	AC-15 AUTOMATED MARKING	AC-15.01-00	See Exhibit F		
			AC-16.01-00	AC-16 SECURITY ATTRIBUTES	AC-16.01-00	See Exhibit F		
				AC-16 SECURITY ATTRIBUTES	Supplemental Guidance	See Exhibit F		
			AC-16(1).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(1).01-00	See Exhibit F		
			AC-16(2).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(2).01-00	See Exhibit F		

			AC-16(3).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(3).01-00	See Exhibit F		
				AC-16 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-16(4).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(4).01-00	See Exhibit F		
				AC-16 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-16(5).01-00	AC-16 CONTROL ENHANCEMENTS	AC-16(5).01-00	See Exhibit F		
				AC-16 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-17.01-00	AC-17 REMOTE ACCESS	AC-17.01-00	See Exhibit F		
			AC-17.01-01	AC-17 REMOTE ACCESS	AC-17.01-01	See Exhibit F		
			AC-17.01-02	AC-17 REMOTE ACCESS	AC-17.01-02	See Exhibit F		
			AC-17.01-03	AC-17 REMOTE ACCESS	AC-17.01-03	See Exhibit F		
			AC-17.01-04	AC-17 REMOTE ACCESS	AC-17.01-04	See Exhibit F		
			AC-17.01-05	AC-17 REMOTE ACCESS	AC-17.01-05	See Exhibit F		
				AC-17 REMOTE ACCESS	Supplemental Guidance	See Exhibit F		
			AC-17(1).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(1).01-00	See Exhibit F		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-17(2).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(2).01-00	See Exhibit F		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-17(3).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(3).01-00	See Exhibit F		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-17(4).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(4).01-00	See Exhibit F		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-17(5).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(5).01-00	See Exhibit F		
			AC-17(6).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(6).01-00	See Exhibit F		
			AC-17(7).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(7).01-00	See Exhibit F		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-17(8).01-00	AC-17 CONTROL ENHANCEMENTS	AC-17(8).01-00	See Exhibit F		
				AC-17 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	See Exhibit F		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	See Exhibit F		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	See Exhibit F		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	See Exhibit F		
			AC-18.01-00	AC-18 WIRELESS ACCESS	AC-18.01-00	See Exhibit F		
				AC-18 WIRELESS ACCESS	Supplemental Guidance	See Exhibit F		
			AC-18(1).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(1).01-00	See Exhibit F		

				AC-18 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-18(2).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(2).01-00	See Exhibit F		
				AC-18 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-18(3).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(3).01-00	See Exhibit F		
			AC-18(4).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(4).01-00	See Exhibit F		
			AC-18(5).01-00	AC-18 CONTROL ENHANCEMENTS	AC-18(5).01-00	See Exhibit F		
				AC-18 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-19.01-00	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-00	See Exhibit F		
			AC-19.01-01	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-01	See Exhibit F		
			AC-19.01-02	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-02	See Exhibit F		
			AC-19.01-03	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-03	See Exhibit F		
			AC-19.01-04	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-04	See Exhibit F		
			AC-19.01-05	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-05	See Exhibit F		
			AC-19.01-06	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-06	See Exhibit F		
			AC-19.01-07	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-07	See Exhibit F		
			AC-19.01-08	AC-19 ACCESS CONTROL FOR MOBILE DEVICES	AC-19.01-08	See Exhibit F		
				AC-19 ACCESS CONTROL FOR MOBILE DEVICES	Supplemental Guidance	See Exhibit F		
				AC-19 ACCESS CONTROL FOR MOBILE DEVICES	Supplemental Guidance	See Exhibit F		
			AC-19(1).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(1).01-00	See Exhibit F		
			AC-19(2).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(2).01-00	See Exhibit F		
			AC-19(3).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(3).01-00	See Exhibit F		
				AC-19 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AC-19(4).01-00	AC-19 CONTROL ENHANCEMENTS	AC-19(4).01-00	See Exhibit F		
			AC-19(4).01-01	AC-19 CONTROL ENHANCEMENTS	AC-19(4).01-01	See Exhibit F		
			AC-19(4).01-02	AC-19 CONTROL ENHANCEMENTS	AC-19(4).01-02	See Exhibit F		
			AC-20.01-00	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	AC-20.01-00	See Exhibit F		
			AC-20.01-01	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	AC-20.01-01	See Exhibit F		
			AC-20.01-02	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	AC-20.01-02	See Exhibit F		
				AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	Enhanced Supplemental	See Exhibit F		
			AC-20(1).01-00	AC-20 CONTROL ENHANCEMENTS	AC-20(1).01-00	See Exhibit F		
			AC-20(1).01-01	AC-20 CONTROL ENHANCEMENTS	AC-20(1).01-01	See Exhibit F		
			AC-20(1).01-02	AC-20 CONTROL ENHANCEMENTS	AC-20(1).01-02	See Exhibit F		
			AC-20(2).01-00	AC-20 CONTROL ENHANCEMENTS	AC-20(2).01-00	See Exhibit F		
				AC-20 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		

			AC-21.01-00	AC-21 USER-BASED COLLABORATION AND	AC-21.01-00	See Exhibit F		
			AC-21.01-01	AC-21 USER-BASED COLLABORATION AND	AC-21.01-01	See Exhibit F		
			AC-21.01-02	AC-21 USER-BASED COLLABORATION AND	AC-21.01-02	See Exhibit F		
				AC-21 USER-BASED COLLABORATION AND	Supplemental Guidance	See Exhibit F		
			AC-21(1).01-00	AC-21 USER-BASED COLLABORATION AND	AC-21(1).01-00	See Exhibit F		
			AC-22.01-00	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-00	See Exhibit F		
			AC-22.01-01	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-01	See Exhibit F		
			AC-22.01-02	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-02	See Exhibit F		
			AC-22.01-03	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-03	See Exhibit F		
			AC-22.01-04	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-04	See Exhibit F		
			AC-22.01-05	AC-22 PUBLICLY ACCESSIBLE CONTENT	AC-22.01-05	See Exhibit F		
				AC-22 PUBLICLY ACCESSIBLE CONTENT	Supplemental Guidance	See Exhibit F		
AT			AT-01.01-00	AT-01 SECURITY AWARENESS AND TRAINING POLICY AND	AT-01.01-00	See Exhibit F		
			AT-01.01-01	AT-01 SECURITY AWARENESS AND TRAINING POLICY AND	AT-01.01-01	See Exhibit F		
			AT-01.01-02	AT-01 SECURITY AWARENESS AND TRAINING POLICY AND	AT-01.01-02	See Exhibit F		
				AT-01 SECURITY AWARENESS AND TRAINING POLICY AND	Supplemental Guidance	See Exhibit F		
			AT-02.01-00	AT-02 SECURITY AWARENESS	AT-02.01-00	See Exhibit F		
				AT-02 SECURITY AWARENESS	Supplemental Guidance	See Exhibit F		
			AT-02(1).01-00	AT-02 CONTROL ENHANCEMENTS	AT-02(1).01-00	See Exhibit F		
				AT-02 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AT-03.01-00	AT-03 SECURITY TRAINING	AT-03.01-00	See Exhibit F		
				AT-03 SECURITY TRAINING	Supplemental Guidance	See Exhibit F		
			AT-03.01-01	AT-03 SECURITY TRAINING	AT-03.01-01	See Exhibit F		
				AT-03 SECURITY TRAINING	Enhanced Supplemental	See Exhibit F		
			AT-03.01-02	AT-03 SECURITY TRAINING	AT-03.01-02	See Exhibit F		
				AT-03 SECURITY TRAINING	Enhanced Supplemental	See Exhibit F		
			AT-04.01-00	AT-04 SECURITY TRAINING RECORDS	AT-04.01-00	See Exhibit F		
			AT-04.01-01	AT-04 SECURITY TRAINING RECORDS	AT-04.01-01	See Exhibit F		
			AT-04.01-02	AT-04 SECURITY TRAINING RECORDS	AT-04.01-02	See Exhibit F		
				AT-04 SECURITY TRAINING RECORDS	Supplemental Guidance	See Exhibit F		
			AT-05.01-00	AT-05 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	AT-05.01-00	See Exhibit F		
				AT-05 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	Supplemental Guidance	See Exhibit F		
AU			AU-01.01-00	AU-01 AUDIT AND ACCOUNTABILITY POLICY AND	AU-01.01-00	See Exhibit F		
			AU-01.01-01	AU-01 AUDIT AND ACCOUNTABILITY POLICY AND	AU-01.01-01	See Exhibit F		

			AU-01.01-02	AU-01 AUDIT AND ACCOUNTABILITY POLICY AND	AU-01.01-02	See Exhibit F		
				AU-01 AUDIT AND ACCOUNTABILITY POLICY AND	Supplemental Guidance	See Exhibit F		
			AU-02.01-00	AU-02 AUDITABLE EVENTS	AU-02.01-00	See Exhibit F		
			AU-02.01-01	AU-02 AUDITABLE EVENTS	AU-02.01-01	See Exhibit F		
			AU-02.01-02	AU-02 AUDITABLE EVENTS	AU-02.01-02	See Exhibit F		
			AU-02.01-03	AU-02 AUDITABLE EVENTS	AU-02.01-03	See Exhibit F		
			AU-02.01-04	AU-02 AUDITABLE EVENTS	AU-02.01-04	See Exhibit F		
				AU-02 AUDITABLE EVENTS	Supplemental Guidance	See Exhibit F		
			AU-02(1).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(1).01-00	See Exhibit F		
			AU-02(2).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(2).01-00	See Exhibit F		
			AU-02(3).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(3).01-00	See Exhibit F		
				AU-02 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-02(4).01-00	AU-02 CONTROL ENHANCEMENTS	AU-02(4).01-00	See Exhibit F		
			AU-03.01-00	AU-03 CONTENT OF AUDIT RECORDS	AU-03.01-00	See Exhibit F		
				AU-03 CONTENT OF AUDIT RECORDS	Supplemental Guidance	See Exhibit F		
			AU-03(1).01-00	AU-03 CONTROL ENHANCEMENTS	AU-03(1).01-00	See Exhibit F		
				AU-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-03(2).01-00	AU-03 CONTROL ENHANCEMENTS	AU-03(2).01-00	See Exhibit F		
			AU-04.01-00	AU-04 AUDIT STORAGE CAPACITY	AU-04.01-00	See Exhibit F		
				AU-04 AUDIT STORAGE CAPACITY	Supplemental Guidance	See Exhibit F		
			AU-05.01-00	AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	AU-05.01-00	See Exhibit F		
			AU-05.01-01	AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	AU-05.01-01	See Exhibit F		
			AU-05.01-02	AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	AU-05.01-02	See Exhibit F		
				AU-05 RESPONSE TO AUDIT PROCESSING FAILURES	Supplemental Guidance	See Exhibit F		
			AU-05(1).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(1).01-00	See Exhibit F		
			AU-05(2).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(2).01-00	See Exhibit F		
			AU-05(3).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(3).01-00	See Exhibit F		
			AU-05(4).01-00	AU-05 CONTROL ENHANCEMENTS	AU-05(4).01-00	See Exhibit F		
			AU-06.01-00	AU-06 AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-06.01-00	See Exhibit F		
			AU-06.01-00	AU-06 AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-06.01-00	See Exhibit F		
			AU-06.01-00	AU-06 AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-06.01-00	See Exhibit F		
			AU-06(1).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(1).01-00	See Exhibit F		
			AU-06(2).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(2).01-00	See Exhibit F		
			AU-06(3).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(3).01-00	See Exhibit F		

			AU-06(4).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(4).01-00	See Exhibit F		
				AU-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-06(5).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(5).01-00	See Exhibit F		
				AU-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-06(6).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(6).01-00	See Exhibit F		
				AU-06 CONTROL ENHANCEMENTS		See Exhibit F		
			AU-06(7).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(7).01-00	See Exhibit F		
				AU-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-06(8).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(8).01-00	See Exhibit F		
			AU-06(9).01-00	AU-06 CONTROL ENHANCEMENTS	AU-06(9).01-00	See Exhibit F		
			AU-07.01-00	AU-07 AUDIT REDUCTION AND REPORT GENERATION	AU-07.01-00	See Exhibit F		
				AU-07 AUDIT REDUCTION AND REPORT GENERATION	Supplemental Guidance	See Exhibit F		
			AU-07(1).01-00	AU-07 CONTROL ENHANCEMENTS	AU-07(1).01-00	See Exhibit F		
			AU-08.01-00	AU-08 TIME STAMPS	AU-08.01-00	See Exhibit F		
				AU-08 TIME STAMPS	Supplemental Guidance	See Exhibit F		
			AU-08(1).01-00	AU-08 CONTROL ENHANCEMENTS	AU-08(1).01-00	See Exhibit F		
			AU-09.01-00	AU-09 PROTECTION OF AUDIT INFORMATION	AU-09.01-00	See Exhibit F		
				AU-09 PROTECTION OF AUDIT INFORMATION	Supplemental Guidance	See Exhibit F		
			AU-09(1).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(1).01-00	See Exhibit F		
			AU-09(2).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(2).01-00	See Exhibit F		
			AU-09(3).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(3).01-00	See Exhibit F		
				AU-09 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-09(4).01-00	AU-09 CONTROL ENHANCEMENTS	AU-09(4).01-00	See Exhibit F		
			AU-09(4).01-01	AU-09 CONTROL ENHANCEMENTS	AU-09(4).01-01	See Exhibit F		
			AU-09(4).01-02	AU-09 CONTROL ENHANCEMENTS	AU-09(4).01-02	See Exhibit F		
				AU-09 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-10.01-00	AU-10 NON-REPUDIATION	AU-10.01-00	See Exhibit F		
				AU-10 NON-REPUDIATION	Supplemental Guidance	See Exhibit F		
			AU-10(1).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(1).01-00	See Exhibit F		
				AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-10(2).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(2).01-00	See Exhibit F		
				AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-10(3).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(3).01-00	See Exhibit F		
				AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		

			AU-10(4).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(4).01-00	See Exhibit F		
				AU-10 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-10(5).01-00	AU-10 CONTROL ENHANCEMENTS	AU-10(5).01-00	See Exhibit F		
			AU-11.01-00	AU-11 AUDIT RECORD RETENTION	AU-11.01-00	See Exhibit F		
				AU-11 AUDIT RECORD RETENTION	Supplemental Guidance	See Exhibit F		
			AU-12.01-00	AU-12 AUDIT GENERATION	AU-12.01-00	See Exhibit F		
			AU-12.01-01	AU-12 AUDIT GENERATION	AU-12.01-01	See Exhibit F		
			AU-12.01-02	AU-12 AUDIT GENERATION	AU-12.01-02	See Exhibit F		
			AU-12.01-03	AU-12 AUDIT GENERATION	AU-12.01-03	See Exhibit F		
				AU-12 AUDIT GENERATION	Supplemental Guidance	See Exhibit F		
			AU-12(1).01-00	AU-12 CONTROL ENHANCEMENTS	AU-12(1).01-00	See Exhibit F		
				AU-12 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-12(2).01-00	AU-12 CONTROL ENHANCEMENTS	AU-12(2).01-00	See Exhibit F		
				AU-12 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			AU-13.01-00	AU-13 MONITORING FOR INFORMATION DISCLOSURE	AU-13.01-00	See Exhibit F		
			AU-14.01-00	AU-14 SESSION AUDIT	AU-14.01-00	See Exhibit F		
			AU-14.01-01	AU-14 SESSION AUDIT	AU-14.01-01	See Exhibit F		
			AU-14.01-02	AU-14 SESSION AUDIT	AU-14.01-02	See Exhibit F		
				AU-14 SESSION AUDIT	Supplemental Guidance	See Exhibit F		
			AU-14(1).01-00	AU-14 CONTROL ENHANCEMENTS	AU-14(1).01-00	See Exhibit F		
CA			CA-01.01-00	CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES	CA-01.01-00	See Exhibit F		
			CA-01.01-01	CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES	CA-01.01-01	See Exhibit F		
			CA-01.01-02	CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES	CA-01.01-02	See Exhibit F		
				CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES	Supplemental Guidance	See Exhibit F		
			CA-02.01-00	CA-02 SECURITY ASSESSMENTS	CA-02.01-00	See Exhibit F		
			CA-02.01-01	CA-02 SECURITY ASSESSMENTS	CA-02.01-01	See Exhibit F		
			CA-02.01-02	CA-02 SECURITY ASSESSMENTS	CA-02.01-02	See Exhibit F		
			CA-02.01-03	CA-02 SECURITY ASSESSMENTS	CA-02.01-03	See Exhibit F		
			CA-02.01-04	CA-02 SECURITY ASSESSMENTS	CA-02.01-04	See Exhibit F		
			CA-02(1).01-00	CA-02 SECURITY ASSESSMENTS	CA-02(1).01-00	See Exhibit F		
				CA-02 SECURITY ASSESSMENTS	Enhanced Supplemental	See Exhibit F		
			CA-02(2).01-00	CA-02 SECURITY ASSESSMENTS	CA-02(2).01-00	See Exhibit F		
				CA-02 SECURITY ASSESSMENTS	Enhanced Supplemental	See Exhibit F		
			CA-03.01-00	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-00	See Exhibit F		

			CA-03.01-01	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-01	See Exhibit F		
			CA-03.01-02	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-02	See Exhibit F		
			CA-03.01-03	CA-03 INFORMATION SYSTEM CONNECTIONS	CA-03.01-03	See Exhibit F		
				CA-03 INFORMATION SYSTEM CONNECTIONS	Supplemental Guidance	See Exhibit F		
			CA-03(1).01-00	CA-03 CONTROL ENHANCEMENTS	CA-03(1).01-00	See Exhibit F		
				CA-03 CONTROL ENHANCEMENTS		See Exhibit F		
			CA-03(2).01-00	CA-03 CONTROL ENHANCEMENTS	CA-03(2).01-00	See Exhibit F		
				CA-03 CONTROL ENHANCEMENTS		See Exhibit F		
			CA-04.01-00	CA-04 SECURITY CERTIFICATION	CA-04.01-00	See Exhibit F		
			CA-05.01-00	CA-05 PLAN OF ACTION AND MILESTONES	CA-05.01-00	See Exhibit F		
			CA-05.01-01	CA-05 PLAN OF ACTION AND MILESTONES	CA-05.01-01	See Exhibit F		
			CA-05.01-02	CA-05 PLAN OF ACTION AND MILESTONES	CA-05.01-02	See Exhibit F		
				CA-05 PLAN OF ACTION AND MILESTONES	Supplemental Guidance	See Exhibit F		
			CA-05(1).01-00	CA-05 CONTROL ENHANCEMENTS	CA-05(1).01-00	See Exhibit F		
			CA-06.01-00	CA-06 SECURITY AUTHORIZATION	CA-06.01-00	See Exhibit F		
			CA-06.01-01	CA-06 SECURITY AUTHORIZATION	CA-06.01-01	See Exhibit F		
			CA-06.01-02	CA-06 SECURITY AUTHORIZATION	CA-06.01-02	See Exhibit F		
			CA-06.01-03	CA-06 SECURITY AUTHORIZATION	CA-06.01-03	See Exhibit F		
			CA-07.01-00	CA-07 CONTINUOUS MONITORING	CA-07.01-00	See Exhibit F		
			CA-07.01-01	CA-07 CONTINUOUS MONITORING	CA-07.01-01	See Exhibit F		
			CA-07.01-02	CA-07 CONTINUOUS MONITORING	CA-07.01-02	See Exhibit F		
			CA-07.01-03	CA-07 CONTINUOUS MONITORING	CA-07.01-03	See Exhibit F		
			CA-07.01-04	CA-07 CONTINUOUS MONITORING	CA-07.01-04	See Exhibit F		
				CA-07 CONTINUOUS MONITORING	Supplemental Guidance	See Exhibit F		
			CA-07(1).01-00	CA-07 CONTROL ENHANCEMENTS	CA-07(1).01-00	See Exhibit F		
				CA-07 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CA-07(2).01-00	CA-07 CONTROL ENHANCEMENTS	CA-07(2).01-00	See Exhibit F		
				CA-07 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
CM			CM-01.01-00	CM-01 CONFIGURATION MANAGEMENT POLICY AND	CM-01.01-00	See Exhibit F		
			CM-01.01-01	CM-01 CONFIGURATION MANAGEMENT POLICY AND	CM-01.01-01	See Exhibit F		
			CM-01.01-02	CM-01 CONFIGURATION MANAGEMENT POLICY AND	CM-01.01-02	See Exhibit F		
				CM-01 CONFIGURATION MANAGEMENT POLICY AND	Supplemental Guidance	See Exhibit F		
			CM-02.01-00	CM-02 BASELINE CONFIGURATION	CM-02.01-00	See Exhibit F		
				CM-02 BASELINE CONFIGURATION	Supplemental Guidance	See Exhibit F		

			CM-02(1).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-00	See Exhibit F		
			CM-02(1).01-01	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-01	See Exhibit F		
			CM-02(1).01-02	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-02	See Exhibit F		
			CM-02(1).01-03	CM-02 CONTROL ENHANCEMENTS	CM-02(1).01-03	See Exhibit F		
			CM-02(2).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(2).01-00	See Exhibit F		
				CM-02 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-02(3).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(3).01-00	See Exhibit F		
			CM-02(4).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(4).01-00	See Exhibit F		
			CM-02(4).01-01	CM-02 CONTROL ENHANCEMENTS	CM-02(4).01-01	See Exhibit F		
			CM-02(4).01-02	CM-02 CONTROL ENHANCEMENTS	CM-02(4).01-02	See Exhibit F		
			CM-02(5).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(5).01-00	See Exhibit F		
			CM-02(5).01-01	CM-02 CONTROL ENHANCEMENTS	CM-02(5).01-01	See Exhibit F		
			CM-02(5).01-02	CM-02 CONTROL ENHANCEMENTS	CM-02(5).01-02	See Exhibit F		
			CM-02(6).01-00	CM-02 CONTROL ENHANCEMENTS	CM-02(6).01-00	See Exhibit F		
			CM-03.01-00	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-00	See Exhibit F		
			CM-03.01-01	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-01	See Exhibit F		
			CM-03.01-02	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-02	See Exhibit F		
			CM-03.01-03	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-03	See Exhibit F		
			CM-03.01-04	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-04	See Exhibit F		
			CM-03.01-05	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-05	See Exhibit F		
			CM-03.01-06	CM-03 CONFIGURATION CHANGE CONTROL	CM-03.01-06	See Exhibit F		
				CM-03 CONFIGURATION CHANGE CONTROL	Supplemental Guidance	See Exhibit F		
			CM-03(1).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-00	See Exhibit F		
			CM-03(1).01-01	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-01	See Exhibit F		
			CM-03(1).01-02	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-02	See Exhibit F		
			CM-03(1).01-03	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-03	See Exhibit F		
			CM-03(1).01-04	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-04	See Exhibit F		
			CM-03(1).01-05	CM-03 CONTROL ENHANCEMENTS	CM-03(1).01-05	See Exhibit F		
			CM-03(2).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(2).01-00	See Exhibit F		
				CM-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-03(3).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(3).01-00	See Exhibit F		
			CM-03(4).01-00	CM-03 CONTROL ENHANCEMENTS	CM-03(4).01-00	See Exhibit F		
				CM-03 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-04.01-00	CM-04 SECURITY IMPACT ANALYSIS	CM-04.01-00	See Exhibit F		

				CM-04 SECURITY IMPACT ANALYSIS	Supplemental Guidance	See Exhibit F		
			CM-04(1).01-00	CM-04 CONTROL ENHANCEMENTS	CM-04(1).01-00	See Exhibit F		
			CM-04(2).01-00	CM-04 CONTROL ENHANCEMENTS	CM-04(2).01-00	See Exhibit F		
			CM-05.01-00	CM-05 ACCESS RESTRICTIONS FOR CHANGE	CM-05.01-00	See Exhibit F		
				CM-05 ACCESS RESTRICTIONS FOR CHANGE	Supplemental Guidance	See Exhibit F		
			CM-05(1).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(1).01-00	See Exhibit F		
			CM-05(2).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(2).01-00	See Exhibit F		
			CM-05(3).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(3).01-00	See Exhibit F		
				CM-05 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-05(4).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(4).01-00	See Exhibit F		
			CM-05(5).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(5).01-00	See Exhibit F		
			CM-05(5).01-01	CM-05 CONTROL ENHANCEMENTS	CM-05(5).01-01	See Exhibit F		
			CM-05(5).01-02	CM-05 CONTROL ENHANCEMENTS	CM-05(5).01-02	See Exhibit F		
			CM-05(6).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(6).01-00	See Exhibit F		
			CM-05(7).01-00	CM-05 CONTROL ENHANCEMENTS	CM-05(7).01-00	See Exhibit F		
				CM-05 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-06.01-00	CM-06 CONFIGURATION SETTINGS	CM-06.01-00	See Exhibit F		
			CM-06.01-01	CM-06 CONFIGURATION SETTINGS	CM-06.01-01	See Exhibit F		
			CM-06.01-02	CM-06 CONFIGURATION SETTINGS	CM-06.01-02	See Exhibit F		
			CM-06.01-03	CM-06 CONFIGURATION SETTINGS	CM-06.01-03	See Exhibit F		
			CM-06.01-04	CM-06 CONFIGURATION SETTINGS	CM-06.01-04	See Exhibit F		
				CM-06 CONFIGURATION SETTINGS	Supplemental Guidance	See Exhibit F		
			CM-06(1).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(1).01-00	See Exhibit F		
			CM-06(2).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(2).01-00	See Exhibit F		
				CM-06 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-06(3).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(3).01-00	See Exhibit F		
			CM-06(4).01-00	CM-06 CONTROL ENHANCEMENTS	CM-06(4).01-00	See Exhibit F		
			CM-07.01-00	CM-07 LEAST FUNCTIONALITY	CM-07.01-00	See Exhibit F		
				CM-07 LEAST FUNCTIONALITY	Supplemental Guidance	See Exhibit F		
			CM-07(1).01-00	CM-07 CONTROL ENHANCEMENTS	CM-07(1).01-00	See Exhibit F		
			CM-07(2).01-00	CM-07 CONTROL ENHANCEMENTS	CM-07(2).01-00	See Exhibit F		
			CM-07(3).01-00	CM-07 CONTROL ENHANCEMENTS	CM-07(3).01-00	See Exhibit F		
				CM-07 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-08.01-00	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-00	See Exhibit F		

			CM-08.01-01	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-01	See Exhibit F		
			CM-08.01-02	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-02	See Exhibit F		
			CM-08.01-03	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-03	See Exhibit F		
			CM-08.01-04	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-04	See Exhibit F		
			CM-08.01-05	CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	CM-08.01-05	See Exhibit F		
				CM-08 INFORMATION SYSTEM COMPONENT INVENTORY	Supplemental Guidance	See Exhibit F		
			CM-08(1).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(1).01-00	See Exhibit F		
			CM-08(2).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(2).01-00	See Exhibit F		
				CM-08 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-08(3).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(3).01-00	See Exhibit F		
			CM-08(3).01-01	CM-08 CONTROL ENHANCEMENTS	CM-08(3).01-01	See Exhibit F		
			CM-08(3).01-02	CM-08 CONTROL ENHANCEMENTS	CM-08(3).01-02	See Exhibit F		
				CM-08 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-08(4).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(4).01-00	See Exhibit F		
			CM-08(5).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(5).01-00	See Exhibit F		
			CM-08(6).01-00	CM-08 CONTROL ENHANCEMENTS	CM-08(6).01-00	See Exhibit F		
				CM-08 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
			CM-09.01-00	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-00	See Exhibit F		
			CM-09.01-01	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-01	See Exhibit F		
			CM-09.01-02	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-02	See Exhibit F		
			CM-09.01-03	CM-09 CONFIGURATION MANAGEMENT PLAN	CM-09.01-03	See Exhibit F		
				CM-09 CONFIGURATION MANAGEMENT PLAN	Supplemental Guidance	See Exhibit F		
			CM-09(1).01-00	CM-09 CONTROL ENHANCEMENTS	CM-09(1).01-00	See Exhibit F		
				CM-09 CONTROL ENHANCEMENTS	Enhanced Supplemental	See Exhibit F		
CP			CP-01.01-00	CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES	CP-01.01-00	See Exhibit F		
			CP-01.01-01		CP-01.01-01	See Exhibit F		
			CP-01.01-02		CP-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			CP-02.01-00	CP-2 CONTINGENCY PLAN	CP-02.01-00	See Exhibit F		
			CP-02.01-01		CP-02.01-01	See Exhibit F		
			CP-02.01-02		CP-02.01-02	See Exhibit F		
			CP-02.01-03		CP-02.01-03	See Exhibit F		
			CP-02.01-04		CP-02.01-04	See Exhibit F		
			CP-02.01-05		CP-02.01-05	See Exhibit F		

			CP-02.01-06		CP-02.01-06	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			CP-02(1).01-00	Control Enhancements:	CP-02(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			CP-02(2).01-00	Control Enhancements:	CP-02(2).01-00	See Exhibit F		
			CP-02(3).01-00	Control Enhancements:	CP-02(3).01-00	See Exhibit F		
			CP-02(4).01-00	Control Enhancements:	CP-02(4).01-00	See Exhibit F		
			CP-02(5).01-00	Control Enhancements:	CP-02(5).01-00	See Exhibit F		
			CP-02(6).01-00	Control Enhancements:	CP-02(6).01-00	See Exhibit F		
			CP-03.01-00	CP-3 CONTINGENCY TRAINING	CP-03.01-00	See Exhibit F		
			CP-03(1).01-00	Control Enhancements:	CP-03(1).01-00	See Exhibit F		
			CP-03(2).01-00	Control Enhancements:	CP-03(2).01-00	See Exhibit F		
			CP-04.01-00	CP-4 CONTINGENCY PLAN TESTING AND EXERCISES	CP-04.01-00	See Exhibit F		
			CP-04.01-01		CP-04.01-01	See Exhibit F		
			CP-04.01-02		CP-04.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			CP-04(1).01-00	Control Enhancements:	CP-04(1).01-00	See Exhibit F		
						See Exhibit F		
			CP-04(2).01-00	Control Enhancements:	CP-04(2).01-00	See Exhibit F		
			CP-04(3).01-00	Control Enhancements:	CP-04(3).01-00	See Exhibit F		
			CP-04(4).01-00	Control Enhancements:	CP-04(4).01-00	See Exhibit F		
			CP-05.01-00	CP-5 CONTINGENCY PLAN UPDATE	CP-05.01-00	See Exhibit F		
			CP-06.01-00	CP-6 ALTERNATE STORAGE SITE	CP-06.01-00	See Exhibit F		
			CP-06(1).01-00	Control Enhancements:	CP-06(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			CP-06(2).01-00	Control Enhancements:	CP-06(2).01-00	See Exhibit F		
			CP-06(3).01-00	Control Enhancements:	CP-06(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			CP-07.01-00	CP-7 ALTERNATE PROCESSING SITE	CP-07.01-00	See Exhibit F		
			CP-07.01-01		CP-07.01-01	See Exhibit F		
			CP-07.01-02		CP-07.01-02	See Exhibit F		
			CP-07(1).01-00	Control Enhancements:	CP-07(1).01-00	See Exhibit F		
						See Exhibit F		
			CP-07(2).01-00	Control Enhancements:	CP-07(2).01-00	See Exhibit F		

			CP-07(3).01-00	Control Enhancements:	CP-07(3).01-00	See Exhibit F		
			CP-07(4).01-00	Control Enhancements:	CP-07(4).01-00	See Exhibit F		
			CP-07(5).01-00	Control Enhancements:	CP-07(5).01-00	See Exhibit F		
			CP-08.01-00	CP-8 TELECOMMUNICATIONS SERVICES	CP-08.01-00	See Exhibit F		
			CP-08(1).01-00	Control Enhancements:	CP-08(1).01-00	See Exhibit F		
			CP-08(1).01-01	Control Enhancements:	CP-08(1).01-01	See Exhibit F		
			CP-08(1).01-02	Control Enhancements:	CP-08(1).01-02	See Exhibit F		
			CP-08(2).01-00	Control Enhancements:	CP-08(2).01-00	See Exhibit F		
			CP-08(3).01-00	Control Enhancements:	CP-08(3).01-00	See Exhibit F		
			CP-08(4).01-00	Control Enhancements:	CP-08(4).01-00	See Exhibit F		
			CP-09.01-00	CP-9 INFORMATION SYSTEM BACKUP	CP-09.01-00	See Exhibit F		
			CP-09.01-01		CP-09.01-01	See Exhibit F		
			CP-09.01-02		CP-09.01-02	See Exhibit F		
			CP-09.01-03		CP-09.01-03	See Exhibit F		
			CP-09.01-04		CP-09.01-04	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			CP-09(1).01-00	Control Enhancements:	CP-09(1).01-00	See Exhibit F		
			CP-09(2).01-00	Control Enhancements:	CP-09(2).01-00	See Exhibit F		
			CP-09(3).01-00	Control Enhancements:	CP-09(3).01-00	See Exhibit F		
			CP-09(4).01-00	Control Enhancements:	CP-09(4).01-00	See Exhibit F		
			CP-09(5).01-00	Control Enhancements:	CP-09(5).01-00	See Exhibit F		
			CP-09(6).01-00	Control Enhancements:	CP-09(6).01-00	See Exhibit F		
			CP-10.01-00	CP-10 INFORMATION SYSTEM RECOVERY AND	CP-10.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			CP-10(1).01-00	Control Enhancements:	CP-10(1).01-00	See Exhibit F		
			CP-10(2).01-00	Control Enhancements:	CP-10(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			CP-10(3).01-00	Control Enhancements:	CP-10(3).01-00	See Exhibit F		
			CP-10(4).01-00	Control Enhancements:	CP-10(4).01-00	See Exhibit F		
			CP-10(5).01-00	Control Enhancements:	CP-10(5).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			CP-10(6).01-00	Control Enhancements:	CP-10(6).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
IA			IA-01.01-00	IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND	IA-01.01-00	See Exhibit F		

			IA-01.01-01		IA-01.01-01	See Exhibit F		
			IA-01.01-02		IA-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			IA-02.01-00	IA-2 IDENTIFICATION AND AUTHENTICATION	IA-02.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			IA-02(1).01-00	Control Enhancements:	IA-02(1).01-00	See Exhibit F		
			IA-02(2).01-00	Control Enhancements:	IA-02(2).01-00	See Exhibit F		
			IA-02(3).01-00	Control Enhancements:	IA-02(3).01-00	See Exhibit F		
			IA-02(4).01-00	Control Enhancements:	IA-02(4).01-00	See Exhibit F		
			IA-02(5).01-00	Control Enhancements:	IA-02(5).01-00	See Exhibit F		
			IA-02(5).01-01	Control Enhancements:	IA-02(5).01-01	See Exhibit F		
			IA-02(5).01-02	Control Enhancements:	IA-02(5).01-02	See Exhibit F		
			IA-02(6).01-00	Control Enhancements:	IA-02(6).01-00	See Exhibit F		
			IA-02(7).01-00	Control Enhancements:	IA-02(7).01-00	See Exhibit F		
			IA-02(8).01-00	Control Enhancements:	IA-02(8).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-02(9).01-00	Control Enhancements:	IA-02(9).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-03.01-00	IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION	IA-03.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			IA-03(1).01-00	Control Enhancements:	IA-03(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-03(2).01-00	Control Enhancements:	IA-03(2).01-00	See Exhibit F		
			IA-03(3).01-00	Control Enhancements:	IA-03(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-04.01-00	IA-4 IDENTIFIER MANAGEMENT	IA-04.01-00	See Exhibit F		
			IA-04.01-01		IA-04.01-01	See Exhibit F		
			IA-04.01-02		IA-04.01-02	See Exhibit F		
			IA-04.01-03		IA-04.01-03	See Exhibit F		
			IA-04.01-04		IA-04.01-04	See Exhibit F		
			IA-04.01-05		IA-04.01-05	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			IA-04(1).01-00	Control Enhancements:	IA-04(1).01-00	See Exhibit F		

					Enhanced Supplemental	See Exhibit F		
			IA-04(2).01-00	Control Enhancements:	IA-04(2).01-00	See Exhibit F		
			IA-04(3).01-00	Control Enhancements:	IA-04(3).01-00	See Exhibit F		
			IA-04(4).01-00	Control Enhancements:	IA-04(4).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-04(5).01-00	Control Enhancements:	IA-04(5).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-05.01-00	IA-5 AUTHENTICATOR MANAGEMENT	IA-05.01-00	See Exhibit F		
			IA-05.01-01		IA-05.01-01	See Exhibit F		
			IA-05.01-02		IA-05.01-02	See Exhibit F		
			IA-05.01-03		IA-05.01-03	See Exhibit F		
			IA-05.01-04		IA-05.01-04	See Exhibit F		
			IA-05.01-05		IA-05.01-05	See Exhibit F		
			IA-05.01-06		IA-05.01-06	See Exhibit F		
			IA-05.01-07		IA-05.01-07	See Exhibit F		
			IA-05.01-08		IA-05.01-08	See Exhibit F		
			IA-05.01-09		IA-05.01-09	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			IA-05(1).01-00	Control Enhancements:	IA-05(1).01-00	See Exhibit F		
			IA-05(1).01-01	Control Enhancements:	IA-05(1).01-01	See Exhibit F		
			IA-05(1).01-02	Control Enhancements:	IA-05(1).01-02	See Exhibit F		
			IA-05(1).01-03	Control Enhancements:	IA-05(1).01-03	See Exhibit F		
			IA-05(1).01-04	Control Enhancements:	IA-05(1).01-04	See Exhibit F		
			IA-05(1).01-05	Control Enhancements:	IA-05(1).01-05	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-05(2).01-00	Control Enhancements:	IA-05(2).01-00	See Exhibit F		
			IA-05(2).01-01	Control Enhancements:	IA-05(2).01-01	See Exhibit F		
			IA-05(2).01-02	Control Enhancements:	IA-05(2).01-02	See Exhibit F		
			IA-05(2).01-03	Control Enhancements:	IA-05(2).01-03	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IA-05(3).01-00	Control Enhancements:	IA-05(3).01-00	See Exhibit F		
			IA-05(4).01-00	Control Enhancements:	IA-05(4).01-00	See Exhibit F		
			IA-05(5).01-00	Control Enhancements:	IA-05(5).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		

			IA-05(6).01-00	Control Enhancements:	IA-05(6).01-00	**See Exhibit F**		
			IA-05(7).01-00	Control Enhancements:	IA-05(7).01-00	**See Exhibit F**		
					Enhanced Supplemental	**See Exhibit F**		
			IA-05(8).01-00	Control Enhancements:	IA-05(8).01-00	**See Exhibit F**		
					Enhanced Supplemental	**See Exhibit F**		
			IA-06.01-00	IA-6 AUTHENTICATOR FEEDBACK	IA-06.01-00	**See Exhibit F**		
					Supplemental Guidance	**See Exhibit F**		
			IA-07.01-00	IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-07.01-00	**See Exhibit F**		
			IA-08.01-00	IA-8 IDENTIFICATION AND AUTHENTICATION (NON-	IA-08.01-00	**See Exhibit F**		
					Supplemental Guidance	**See Exhibit F**		
IR			IR-01.01-00	IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES	IR-01.01-00	**See Exhibit F**		
			IR-01.01-01		IR-01.01-01	**See Exhibit F**		
			IR-01.01-02		IR-01.01-02	**See Exhibit F**		
					Supplemental Guidance	**See Exhibit F**		
			IR-02.01-00	IR-2 INCIDENT RESPONSE TRAINING	IR-02.01-00	**See Exhibit F**		
			IR-02.01-01		IR-02.01-01	**See Exhibit F**		
			IR-02.01-02		IR-02.01-02	**See Exhibit F**		
						See Exhibit F		
			IR-02(1).01-00	Control Enhancements:	IR-02(1).01-00	**See Exhibit F**		
			IR-02(2).01-00	Control Enhancements:	IR-02(2).01-00	**See Exhibit F**		
			IR-03.01-00	IR-3 INCIDENT RESPONSE TESTING AND EXERCISES	IR-03.01-00	**See Exhibit F**		
			IR-03(1).01-00	Control Enhancements:	IR-03(1).01-00	**See Exhibit F**		
					Enhanced Supplemental	**See Exhibit F**		
			IR-04.01-00	IR-4 INCIDENT HANDLING	IR-04.01-00	**See Exhibit F**		
			IR-04.01-01		IR-04.01-01	**See Exhibit F**		
			IR-04.01-02		IR-04.01-02	**See Exhibit F**		
			IR-04.01-03		IR-04.01-03	**See Exhibit F**		
					Supplemental Guidance	**See Exhibit F**		
			IR-04(1).01-00	Control Enhancements:	IR-04(1).01-00	**See Exhibit F**		
						See Exhibit F		
			IR-04(2).01-00	Control Enhancements:	IR-04(2).01-00	**See Exhibit F**		
						See Exhibit F		
			IR-04(3).01-00	Control Enhancements:	IR-04(3).01-00	**See Exhibit F**		
					Enhanced Supplemental	**See Exhibit F**		

			IR-04(4).01-00	Control Enhancements:	IR-04(4).01-00	See Exhibit F		
			IR-04(5).01-00	Control Enhancements:	IR-04(5).01-00	See Exhibit F		
			IR-05.01-00	IR-5 INCIDENT MONITORING	IR-05.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			IR-05(1).01-00	Control Enhancements:	IR-05(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IR-06.01-00	IR-6 INCIDENT REPORTING	IR-06.01-00	See Exhibit F		
			IR-06.01-01		IR-06.01-01	See Exhibit F		
			IR-06.01-02		IR-06.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			IR-06(1).01-00	Control Enhancements:	IR-06(1).01-00	See Exhibit F		
			IR-06(2).01-00	Control Enhancements:	IR-06(2).01-00	See Exhibit F		
			IR-07.01-00	IR-7 INCIDENT RESPONSE ASSISTANCE	IR-07.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			IR-07(1).01-00	Control Enhancements:	IR-07(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IR-07(2).01-00	Control Enhancements:	IR-07(2).01-00	See Exhibit F		
			IR-07(2).01-01	Control Enhancements:	IR-07(2).01-01	See Exhibit F		
			IR-07(2).01-02	Control Enhancements:	IR-07(2).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			IR-08.01-00	IR-8 INCIDENT RESPONSE PLAN	IR-08.01-00	See Exhibit F		
			IR-08.01-01		IR-08.01-01	See Exhibit F		
			IR-08.01-02		IR-08.01-02	See Exhibit F		
			IR-08.01-03		IR-08.01-03	See Exhibit F		
			IR-08.01-04		IR-08.01-04	See Exhibit F		
			IR-08.01-05		IR-08.01-05	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
MA			MA-01.01-00	MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES	MA-01.01-00	See Exhibit F		
			MA-01.01-01		MA-01.01-01	See Exhibit F		
			MA-01.01-02		MA-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MA-02.01-00	MA-2 CONTROLLED MAINTENANCE	MA-02.01-00	See Exhibit F		

			MA-02.01-01		MA-02.01-01	See Exhibit F		
			MA-02.01-02		MA-02.01-02	See Exhibit F		
			MA-02.01-03		MA-02.01-03	See Exhibit F		
			MA-02.01-04		MA-02.01-04	See Exhibit F		
			MA-02.01-05		MA-02.01-05	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MA-02(1).01-00	Control Enhancements:	MA-02(1).01-00	See Exhibit F		
			MA-02(1).01-01	Control Enhancements:	MA-02(1).01-01	See Exhibit F		
			MA-02(1).01-02	Control Enhancements:	MA-02(1).01-02	See Exhibit F		
			MA-02(1).01-03	Control Enhancements:	MA-02(1).01-03	See Exhibit F		
			MA-02(1).01-04	Control Enhancements:	MA-02(1).01-04	See Exhibit F		
			MA-02(1).01-05	Control Enhancements:	MA-02(1).01-05	See Exhibit F		
			MA-02(2).01-00	Control Enhancements:	MA-02(2).01-00	See Exhibit F		
			MA-03.01-00	MA-3 MAINTENANCE TOOLS	MA-03.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MA-03(1).01-00	Control Enhancements:	MA-03(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			MA-03(2).01-00	Control Enhancements:	MA-03(2).01-00	See Exhibit F		
			MA-03(3).01-00	Control Enhancements:	MA-03(3).01-00	See Exhibit F		
			MA-03(4).01-00	Control Enhancements:	MA-03(4).01-00	See Exhibit F		
			MA-04.01-00	MA-4 NON-LOCAL MAINTENANCE	MA-04.01-00	See Exhibit F		
			MA-04.01-01		MA-04.01-01	See Exhibit F		
			MA-04.01-02		MA-04.01-02	See Exhibit F		
			MA-04.01-03		MA-04.01-03	See Exhibit F		
			MA-04.01-04		MA-04.01-04	See Exhibit F		
			MA-04.01-05		MA-04.01-05	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MA-04(1).01-00	Control Enhancements:	MA-04(1).01-00	See Exhibit F		
			MA-04(2).01-00	Control Enhancements:	MA-04(2).01-00	See Exhibit F		
			MA-04(3).01-00	Control Enhancements:	MA-04(3).01-00	See Exhibit F		
			MA-04(3).01-01	Control Enhancements:	MA-04(3).01-01	See Exhibit F		
			MA-04(3).01-02	Control Enhancements:	MA-04(3).01-02	See Exhibit F		
			MA-04(4).01-00	Control Enhancements:	MA-04(4).01-00	See Exhibit F		
			MA-04(4).01-01	Control Enhancements:	MA-04(4).01-01	See Exhibit F		

			MA-04(4).01-02	Control Enhancements:	MA-04(4).01-02	See Exhibit F		
			MA-04(5).01-00	Control Enhancements:	MA-04(5).01-00	See Exhibit F		
			MA-04(5).01-01	Control Enhancements:	MA-04(5).01-01	See Exhibit F		
			MA-04(5).01-02	Control Enhancements:	MA-04(5).01-02	See Exhibit F		
			MA-04(6).01-00	Control Enhancements:	MA-04(6).01-00	See Exhibit F		
			MA-04(7).01-00	Control Enhancements:	MA-04(7).01-00	See Exhibit F		
			MA-05.01-00	MA-5 MAINTENANCE PERSONNEL	MA-05.01-00	See Exhibit F		
			MA-05.01-01		MA-05.01-01	See Exhibit F		
			MA-05.01-02		MA-05.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MA-05(1).01-00	Control Enhancements:	MA-05(1).01-00	See Exhibit F		
			MA-05(1).01-01	Control Enhancements:	MA-05(1).01-01	See Exhibit F		
			MA-05(1).01-02	Control Enhancements:	MA-05(1).01-02	See Exhibit F		
			MA-05(1).01-03	Control Enhancements:	MA-05(1).01-03	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			MA-05(2).01-00	Control Enhancements:	MA-05(2).01-00	See Exhibit F		
			MA-05(3).01-00	Control Enhancements:	MA-05(3).01-00	See Exhibit F		
			MA-05(4).01-00	Control Enhancements:	MA-05(4).01-00	See Exhibit F		
			MA-05(4).01-01	Control Enhancements:	MA-05(4).01-01	See Exhibit F		
			MA-05(4).01-02	Control Enhancements:	MA-05(4).01-02	See Exhibit F		
			MA-06.01-00	MA-6 TIMELY MAINTENANCE	MA-06.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
MP			MP-01.01-00	MP-1 MEDIA PROTECTION POLICY AND PROCEDURES	MP-01.01-00	See Exhibit F		
			MP-01.01-01		MP-01.01-01	See Exhibit F		
			MP-01.01-02		MP-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MP-02.01-00	MP-2 MEDIA ACCESS	MP-02.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MP-02(1).01-00	Control Enhancements:	MP-02(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			MP-02(2).01-00		MP-02(2).01-00	See Exhibit F		
			MP-03.01-00	MP-3 MEDIA MARKING	MP-03.01-00	See Exhibit F		
			MP-03.01-01		MP-03.01-01	See Exhibit F		
			MP-03.01-02		MP-03.01-02	See Exhibit F		

					Supplemental Guidance	See Exhibit F		
			MP-04.01-00	MP-4 MEDIA STORAGE	MP-04.01-00	See Exhibit F		
			MP-04.01-01		MP-04.01-01	See Exhibit F		
			MP-04.01-02		MP-04.01-02	See Exhibit F		
			MP-04(1).01-00	Control Enhancements:	MP-04(1).01-00	See Exhibit F		
			MP-05.01-00	MP-5 MEDIA TRANSPORT	MP-05.01-00	See Exhibit F		
			MP-05.01-01		MP-05.01-01	See Exhibit F		
			MP-05.01-02		MP-05.01-02	See Exhibit F		
			MP-05.01-03		MP-05.01-03	See Exhibit F		
						See Exhibit F		
			MP-05(1).01-00	Control Enhancements:	MP-05(1).01-00	See Exhibit F		
			MP-05(2).01-00	Control Enhancements:	MP-05(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			MP-05(3).01-00	Control Enhancements:	MP-05(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			MP-05(4).01-00	Control Enhancements:	MP-05(4).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			MP-06.01-00	MP-6 MEDIA SANITIZATION	MP-06.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			MP-06(1).01-00	Control Enhancements:	MP-06(1).01-00	See Exhibit F		
			MP-06(2).01-00	Control Enhancements:	MP-06(2).01-00	See Exhibit F		
			MP-06(3).01-00	Control Enhancements:	MP-06(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			MP-06(4).01-00	Control Enhancements:	MP-06(4).01-00	See Exhibit F		
			MP-06(5).01-00	Control Enhancements:	MP-06(5).01-00	See Exhibit F		
			MP-06(6).01-00	Control Enhancements:	MP-06(6).01-00	See Exhibit F		
PE			PE-01.01-00	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-01.01-00	See Exhibit F		
			PE-01.01-01		PE-01.01-01	See Exhibit F		
			PE-01.01-02		PE-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-02.01-00	PE-2 PHYSICAL ACCESS AUTHORIZATIONS	PE-02.01-00	See Exhibit F		
			PE-02.01-01		PE-02.01-01	See Exhibit F		
			PE-02.01-02		PE-02.01-02	See Exhibit F		
			PE-02.01-03		PE-02.01-03	See Exhibit F		

					Supplemental Guidance	See Exhibit F		
			PE-02(1).01-00	Control Enhancements:	PE-02(1).01-00	See Exhibit F		
			PE-02(2).01-00	Control Enhancements:	PE-02(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			PE-02(3).01-00	Control Enhancements:	PE-02(3).01-00	See Exhibit F		
			PE-03.01-00	PE-3 PHYSICAL ACCESS CONTROL	PE-03.01-00	See Exhibit F		
			PE-03.01-01		PE-03.01-01	See Exhibit F		
			PE-03.01-02		PE-03.01-02	See Exhibit F		
			PE-03.01-03		PE-03.01-03	See Exhibit F		
			PE-03.01-04		PE-03.01-04	See Exhibit F		
			PE-03.01-05		PE-03.01-05	See Exhibit F		
			PE-03.01-06		PE-03.01-06	See Exhibit F		
			PE-03.01-07		PE-03.01-07	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-03(1).01-00	Control Enhancements:	PE-03(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			PE-03(2).01-00	Control Enhancements:	PE-03(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			PE-03(3).01-00	Control Enhancements:	PE-03(3).01-00	See Exhibit F		
			PE-03(4).01-00	Control Enhancements:	PE-03(4).01-00	See Exhibit F		
			PE-03(5).01-00	Control Enhancements:	PE-03(5).01-00	See Exhibit F		
			PE-03(6).01-00	Control Enhancements:	PE-03(6).01-00	See Exhibit F		
			PE-04.01-00	PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM	PE-04.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-05.01-00	PE-5 ACCESS CONTROL FOR OUTPUT DEVICES	PE-05.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-06.01-00	PE-6 MONITORING PHYSICAL ACCESS	PE-06.01-00	See Exhibit F		
			PE-06.01-01		PE-06.01-01	See Exhibit F		
			PE-06.01-02		PE-06.01-02	See Exhibit F		
			PE-06.01-03		PE-06.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			PE-06(1).01-00	Control Enhancements:	PE-06(1).01-00	See Exhibit F		
			PE-06(2).01-00	Control Enhancements:	PE-06(2).01-00	See Exhibit F		

			PE-07.01-00	PE-7 VISITOR CONTROL	PE-07.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-07(1).01-00	Control Enhancements:	PE-07(1).01-00	See Exhibit F		
			PE-07(2).01-00	Control Enhancements:	PE-07(2).01-00	See Exhibit F		
			PE-08.01-00	PE-8 ACCESS RECORDS	PE-08.01-00	See Exhibit F		
			PE-08.01-01		PE-08.01-01	See Exhibit F		
			PE-08.01-02		PE-08.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-08(1).01-00	Control Enhancements:	PE-08(1).01-00	See Exhibit F		
			PE-08(2).01-00	Control Enhancements:	PE-08(2).01-00	See Exhibit F		
			PE-09.01-00	PE-9 POWER EQUIPMENT AND POWER CABLING	PE-09.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-09(1).01-00	Control Enhancements:	PE-09(1).01-00	See Exhibit F		
			PE-09(2).01-00	Control Enhancements:	PE-09(2).01-00	See Exhibit F		
			PE-10.01-00	PE-10 EMERGENCY SHUTOFF	PE-10.01-00	See Exhibit F		
			PE-10.01-01		PE-10.01-01	See Exhibit F		
			PE-10.01-02		PE-10.01-02	See Exhibit F		
			PE-10.01-03		PE-10.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-10(1).01-00	Control Enhancements:	PE-10(1).01-00	See Exhibit F		
			PE-11.01-00	PE-11 EMERGENCY POWER	PE-11.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-11(1).01-01	Control Enhancements:	PE-11(1).01-01	See Exhibit F		
			PE-11(1).01-02	Control Enhancements:	PE-11(1).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			PE-12.01-00	PE-12 EMERGENCY LIGHTING	PE-12.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-12(1).01-00	Control Enhancements:	PE-12(1).01-00	See Exhibit F		
			PE-13.01-00	PE-13 FIRE PROTECTION	PE-13.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-13(1).01-00	Control Enhancements:	PE-13(1).01-00	See Exhibit F		
			PE-13(2).01-00	Control Enhancements:	PE-13(2).01-00	See Exhibit F		
			PE-13(3).01-00	Control Enhancements:	PE-13(3).01-00	See Exhibit F		
			PE-13(4).01-00	Control Enhancements:	PE-13(4).01-00	See Exhibit F		

			PE-14.01-00	PE-14 TEMPERATURE AND HUMIDITY CONTROLS	PE-14.01-00	See Exhibit F		
			PE-14.01-01		PE-14.01-01	See Exhibit F		
			PE-14.01-02		PE-14.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-14(1).01-01	Control Enhancements:	PE-14(1).01-01	See Exhibit F		
			PE-14(2).01-02	Control Enhancements:	PE-14(2).01-02	See Exhibit F		
			PE-15.01-00	PE-15 WATER DAMAGE PROTECTION	PE-15.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-15(1).01-00	Control Enhancements:	PE-15(1).01-00	See Exhibit F		
			PE-16.01-00	PE-16 DELIVERY AND REMOVAL	PE-16.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-17.01-00	PE-17 ALTERNATE WORK SITE	PE-17.01-00	See Exhibit F		
			PE-17.01-01		PE-17.01-01	See Exhibit F		
			PE-17.01-02		PE-17.01-02	See Exhibit F		
			PE-17.01-03		PE-17.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-18.01-00	PE-18 LOCATION OF INFORMATION SYSTEM	PE-18.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PE-18(1).01-00	Control Enhancements:	PE-18(1).01-00	See Exhibit F		
			PE-19.01-00	PE-19 INFORMATION LEAKAGE	PE-19.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			PE-19(1).01-00	Control Enhancements:	PE-19(1).01-00	See Exhibit F		
PL			PL-01.01-00	PL-1 SECURITY PLANNING POLICY AND PROCEDURES	PL-01.01-00	See Exhibit F		
			PL-01.01-01		PL-01.01-01	See Exhibit F		
			PL-01.01-02		PL-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PL-02.01-00	PL-2 SYSTEM SECURITY PLAN	PL-02.01-00	See Exhibit F		
			PL-02.01-00		PL-02.01-00	See Exhibit F		
			PL-02.01-01		PL-02.01-01	See Exhibit F		
			PL-02.01-02		PL-02.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			PL-02(1).01-00	Control Enhancements:	PL-02(1).01-00	See Exhibit F		

			PL-02(1).01-01	Control Enhancements:	PL-02(1).01-01	See Exhibit F		
			PL-02(1).01-02	Control Enhancements:	PL-02(1).01-02	See Exhibit F		
						See Exhibit F		
			PL-02(2).01-00	Control Enhancements:	PL-02(2).01-00	See Exhibit F		
			PL-02(2).01-01	Control Enhancements:	PL-02(2).01-01	See Exhibit F		
			PL-02(2).01-02	Control Enhancements:	PL-02(2).01-02	See Exhibit F		
			PL-02(2).01-03	Control Enhancements:	PL-02(2).01-03	See Exhibit F		
			PL-02(2).01-04	Control Enhancements:	PL-02(2).01-04	See Exhibit F		
			PL-02(2).01-05	Control Enhancements:	PL-02(2).01-05	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			PL-03.01-00	PL-3 SYSTEM SECURITY PLAN UPDATE	PL-03.01-00	See Exhibit F		
			PL-04.01-00	PL-4 RULES OF BEHAVIOR	PL-04.01-00	See Exhibit F		
			PL-04.01-01		PL-04.01-01	See Exhibit F		
			PL-04.01-02		PL-04.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PL-04(1).01-00	Control Enhancements:	PL-04(1).01-00	See Exhibit F		
			PL-05.01-00	PL-5 PRIVACY IMPACT ASSESSMENT	PL-05.01-00	See Exhibit F		
			PL-06.01-00	PL-6 SECURITY-RELATED ACTIVITY PLANNING	PL-06.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PS-01.01-00	PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES	PS-01.01-00	See Exhibit F		
			PS-01.01-01		PS-01.01-01	See Exhibit F		
			PS-01.01-02		PS-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
PS			PS-02.01-00	PS-2 POSITION CATEGORIZATION	PS-02.01-00	See Exhibit F		
			PS-02.01-01		PS-02.01-01	See Exhibit F		
			PS-02.01-02		PS-02.01-02	See Exhibit F		
			PS-02.01-03		PS-02.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PS-03.01-00	PS-3 PERSONNEL SCREENING	PS-03.01-00	See Exhibit F		
			PS-03.01-01		PS-03.01-01	See Exhibit F		
			PS-03.01-02		PS-03.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PS-03(1).01-00	Control Enhancements:	PS-03(1).01-00	See Exhibit F		
			PS-03(2).01-00	Control Enhancements:	PS-03(2).01-00	See Exhibit F		

					Enhanced Supplemental	See Exhibit F		
			PS-04.01-00	PS-4 PERSONNEL TERMINATION	PS-04.01-00	See Exhibit F		
			PS-04.01-01		PS-04.01-01	See Exhibit F		
			PS-04.01-02		PS-04.01-02	See Exhibit F		
			PS-04.01-03		PS-04.01-03	See Exhibit F		
			PS-04.01-04		PS-04.01-04	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PS-05.01-00	PS-5 PERSONNEL TRANSFER	PS-05.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PS-06.01-00	PS-6 ACCESS AGREEMENTS	PS-06.01-00	See Exhibit F		
			PS-06.01-01		PS-06.01-01	See Exhibit F		
			PS-06.01-02		PS-06.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			PS-06(1).01-00	Control Enhancements:	PS-06(1).01-00	See Exhibit F		
			PS-06(1).01-01	Control Enhancements:	PS-06(1).01-01	See Exhibit F		
			PS-06(1).01-02	Control Enhancements:	PS-06(1).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			PS-06(2).01-00	Control Enhancements:	PS-06(2).01-00	See Exhibit F		
			PS-06(2).01-01	Control Enhancements:	PS-06(2).01-01	See Exhibit F		
			PS-06(2).01-02	Control Enhancements:	PS-06(2).01-02	See Exhibit F		
			PS-06(2).01-03	Control Enhancements:	PS-06(2).01-03	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			PS-07.01-00	PS-7 THIRD-PARTY PERSONNEL SECURITY	PS-07.01-00	See Exhibit F		
			PS-07.01-01		PS-07.01-01	See Exhibit F		
			PS-07.01-02		PS-07.01-02	See Exhibit F		
			PS-07.01-03		PS-07.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PS-08.01-00	PS-8 PERSONNEL SANCTIONS	PS-08.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			RA-01.01-00	RA-1 RISK ASSESSMENT POLICY AND PROCEDURES	RA-01.01-00	See Exhibit F		
			RA-01.01-01		RA-01.01-01	See Exhibit F		
			RA-01.01-02		RA-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		

RA			RA-02.01-00	RA-2 SECURITY CATEGORIZATION	RA-02.01-00	See Exhibit F		
			RA-02.01-01		RA-02.01-01	See Exhibit F		
			RA-02.01-02		RA-02.01-02	See Exhibit F		
			RA-02.01-03		RA-02.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			RA-03.01-00	RA-3 RISK ASSESSMENT	RA-03.01-00	See Exhibit F		
			RA-03.01-01		RA-03.01-01	See Exhibit F		
			RA-03.01-02		RA-03.01-02	See Exhibit F		
			RA-03.01-03		RA-03.01-03	See Exhibit F		
			RA-03.01-04		RA-03.01-04	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			RA-04.01-00	RA-4 RISK ASSESSMENT UPDATE	RA-04.01-00	See Exhibit F		
			RA-05.01-00	RA-5 VULNERABILITY SCANNING	RA-05.01-00	See Exhibit F		
			RA-05.01-01		RA-05.01-01	See Exhibit F		
			RA-05.01-02		RA-05.01-02	See Exhibit F		
			RA-05.01-03		RA-05.01-03	See Exhibit F		
			RA-05.01-04		RA-05.01-04	See Exhibit F		
			RA-05.01-05		RA-05.01-05	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			RA-05(1).01-00	Control Enhancements:	RA-05(1).01-00	See Exhibit F		
			RA-05(2).01-00	Control Enhancements:	RA-05(2).01-00	See Exhibit F		
			RA-05(3).01-00	Control Enhancements:	RA-05(3).01-00	See Exhibit F		
			RA-05(4).01-00	Control Enhancements:	RA-05(4).01-00	See Exhibit F		
			RA-05(5).01-00	Control Enhancements:	RA-05(5).01-00	See Exhibit F		
			RA-05(6).01-00	Control Enhancements:	RA-05(6).01-00	See Exhibit F		
			RA-05(7).01-00	Control Enhancements:	RA-05(7).01-00	See Exhibit F		
			RA-05(8).01-00	Control Enhancements:	RA-05(8).01-00	See Exhibit F		
			RA-05(9).01-00	Control Enhancements:	RA-05(9).01-00	See Exhibit F		
			RA-05(9).01-00	Control Enhancements:	RA-05(9).01-00	See Exhibit F		
			RA-05(9).01-00	Control Enhancements:	RA-05(9).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
SA			SA-01.01-00	SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND	SA-01.01-00	See Exhibit F		
			SA-01.01-01		SA-01.01-01	See Exhibit F		

			SA-01.01-02		SA-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-02.01-00	SA-2 ALLOCATION OF RESOURCES	SA-02.01-00	See Exhibit F		
			SA-02.01-01		SA-02.01-01	See Exhibit F		
			SA-02.01-02		SA-02.01-02	See Exhibit F		
			SA-02.01-03		SA-02.01-03	See Exhibit F		
			SA-03.01-00	SA-3 LIFE CYCLE SUPPORT	SA-03.01-00	See Exhibit F		
			SA-03.01-01		SA-03.01-01	See Exhibit F		
			SA-03.01-02		SA-03.01-02	See Exhibit F		
			SA-03.01-03		SA-03.01-03	See Exhibit F		
			SA-04.01-00	SA-4 ACQUISITIONS	SA-04.01-00	See Exhibit F		
			SA-04.01-01		SA-04.01-01	See Exhibit F		
			SA-04.01-02		SA-04.01-02	See Exhibit F		
			SA-04.01-03		SA-04.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-04(1).01-00	Control Enhancements:	SA-04(1).01-00	See Exhibit F		
			SA-04(2).01-00	Control Enhancements:	SA-04(2).01-00	See Exhibit F		
			SA-04(3).01-00	Control Enhancements:	SA-04(3).01-00	See Exhibit F		
			SA-04(4).01-00	Control Enhancements:	SA-04(4).01-00	See Exhibit F		
			SA-04(5).01-00	Control Enhancements:	SA-04(5).01-00	See Exhibit F		
			SA-04(6).01-00	Control Enhancements:	SA-04(6).01-00	See Exhibit F		
			SA-04(6).01-01	Control Enhancements:	SA-04(6).01-01	See Exhibit F		
			SA-04(6).01-02	Control Enhancements:	SA-04(6).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-04(7).01-00	Control Enhancements:	SA-04(7).01-00	See Exhibit F		
			SA-04(7).01-01	Control Enhancements:	SA-04(7).01-01	See Exhibit F		
			SA-04(7).01-02	Control Enhancements:	SA-04(7).01-02	See Exhibit F		
			SA-05.01-00	SA-5 INFORMATION SYSTEM DOCUMENTATION	SA-05.01-00	See Exhibit F		
			SA-05.01-01		SA-05.01-01	See Exhibit F		
			SA-05.01-02		SA-05.01-02	See Exhibit F		
			SA-05.01-03		SA-05.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			SA-05(1).01-00	Control Enhancements:	SA-05(1).01-00	See Exhibit F		

			SA-05(2).01-00	Control Enhancements:	SA-05(2).01-00	See Exhibit F		
			SA-05(3).01-00	Control Enhancements:	SA-05(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-05(4).01-00	Control Enhancements:	SA-05(4).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-05(5).01-00	Control Enhancements:	SA-05(5).01-00	See Exhibit F		
			SA-06.01-00	SA-6 SOFTWARE USAGE RESTRICTIONS	SA-06.01-00	See Exhibit F		
			SA-06.01-01		SA-06.01-01	See Exhibit F		
			SA-06.01-02		SA-06.01-02	See Exhibit F		
			SA-06.01-03		SA-06.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-06(1).01-00	Control Enhancements:	SA-06(1).01-00	See Exhibit F		
			SA-06(1).01-01		SA-06(1).01-01	See Exhibit F		
			SA-06(1).01-02		SA-06(1).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-07.01-00	SA-7 USER-INSTALLED SOFTWARE	SA-07.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-08.01-00	SA-8 SECURITY ENGINEERING PRINCIPLES	SA-08.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-09.01-00	SA-9 EXTERNAL INFORMATION SYSTEM SERVICES	SA-09.01-00	See Exhibit F		
			SA-09.01-01		SA-09.01-01	See Exhibit F		
			SA-09.01-02		SA-09.01-02	See Exhibit F		
			SA-09.01-03		SA-09.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-09(1).01-00	Control Enhancements:	SA-09(1).01-00	See Exhibit F		
			SA-09(1).01-01	Control Enhancements:	SA-09(1).01-01	See Exhibit F		
			SA-09(1).01-02	Control Enhancements:	SA-09(1).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-10.01-00	SA-10 DEVELOPER CONFIGURATION MANAGEMENT	SA-10.01-00	See Exhibit F		
			SA-10.01-01		SA-10.01-01	See Exhibit F		
			SA-10.01-02		SA-10.01-02	See Exhibit F		
			SA-10.01-03		SA-10.01-03	See Exhibit F		
			SA-10.01-04		SA-10.01-04	See Exhibit F		
			SA-10.01-05		SA-10.01-05	See Exhibit F		

						See Exhibit F		
			SA-10(1).01-00	Control Enhancements:	SA-10(1).01-00	See Exhibit F		
			SA-10(2).01-00	Control Enhancements:	SA-10(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-11.01-00	SA-11 DEVELOPER SECURITY TESTING	SA-11.01-00	See Exhibit F		
			SA-11.01-01		SA-11.01-01	See Exhibit F		
			SA-11.01-02		SA-11.01-02	See Exhibit F		
			SA-11.01-03		SA-11.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-11(1).01-00	Control Enhancements:	SA-11(1).01-00	See Exhibit F		
			SA-11(2).01-00	Control Enhancements:	SA-11(2).01-00	See Exhibit F		
			SA-11(3).01-00	Control Enhancements:	SA-11(3).01-00	See Exhibit F		
			SA-12.01-00	SA-12 SUPPLY CHAIN PROTECTION	SA-12.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-12(1).01-00	Control Enhancements:	SA-12(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-12(2).01-00	Control Enhancements:	SA-12(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-12(3).01-00	Control Enhancements:	SA-12(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-12(4).01-00	Control Enhancements:	SA-12(4).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-12(5).01-00	Control Enhancements:	SA-12(5).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-12(6).01-00	Control Enhancements:	SA-12(6).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SA-12(7).01-00	Control Enhancements:	SA-12(7).01-00	See Exhibit F		
			SA-13.01-00	SA-13 TRUSTWORTHINESS	SA-13.01-00	See Exhibit F		
			SA-14.01-00	SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS	SA-14.01-00	See Exhibit F		
			SA-14.01-01		SA-14.01-01	See Exhibit F		
			SA-14.01-02		SA-14.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SA-14(1).01-00	Control Enhancements:	SA-14(1).01-00	See Exhibit F		
			SA-14(1).01-01	Control Enhancements:	SA-14(1).01-01	See Exhibit F		

			SA-14(1).01-02	Control Enhancements:	SA-14(1).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
SC			SC-01.01-00	SC-1 SYSTEM AND COMMUNICATIONS PROTECTION	SC-01.01-00	See Exhibit F		
			SC-01.01-01		SC-01.01-01	See Exhibit F		
			SC-01.01-02		SC-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-02.01-00	SC-2 APPLICATION PARTITIONING	SC-02.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-02(1).01-00	Control Enhancements:	SC-02(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-03.01-00	SC-3 SECURITY FUNCTION ISOLATION	SC-03.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-03(1).01-00	Control Enhancements:	SC-03(1).01-00	See Exhibit F		
			SC-03(2).01-00	Control Enhancements:	SC-03(2).01-00	See Exhibit F		
			SC-03(3).01-00	Control Enhancements:	SC-03(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-03(4).01-00		SC-03(4).01-00	See Exhibit F		
			SC-03(5).01-00		SC-03(5).01-00	See Exhibit F		
			SC-04.01-00	SC-4 INFORMATION IN SHARED RESOURCES	SC-04.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-04(1).01-00	Control Enhancements:	SC-04(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-05.01-00	SC-5 DENIAL OF SERVICE PROTECTION	SC-05.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-05(1).01-00	Control Enhancements:	SC-05(1).01-00	See Exhibit F		
			SC-05(2).01-00	Control Enhancements:	SC-05(2).01-00	See Exhibit F		
			SC-06.01-00	SC-6 RESOURCE PRIORITY	SC-06.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-07.01-00	SC-7 BOUNDARY PROTECTION	SC-07.01-00	See Exhibit F		
			SC-07.01-01		SC-07.01-01	See Exhibit F		
			SC-07.01-02		SC-07.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-07(1).01-00	Control Enhancements:	SC-07(1).01-00	See Exhibit F		

					Enhanced Supplemental	See Exhibit F			
			SC-07(2).01-00	Control Enhancements:	SC-07(2).01-00	See Exhibit F			
			SC-07(3).01-00	Control Enhancements:	SC-07(3).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(4).01-00	Control Enhancements:	SC-07(4).01-00	See Exhibit F			
			SC-07(4).01-01	Control Enhancements:	SC-07(4).01-01	See Exhibit F			
			SC-07(4).01-02	Control Enhancements:	SC-07(4).01-02	See Exhibit F			
			SC-07(4).01-03	Control Enhancements:	SC-07(4).01-03	See Exhibit F			
			SC-07(4).01-04	Control Enhancements:	SC-07(4).01-04	See Exhibit F			
			SC-07(4).01-05	Control Enhancements:	SC-07(4).01-05	See Exhibit F			
			SC-07(4).01-06	Control Enhancements:	SC-07(4).01-06	See Exhibit F			
			SC-07(5).01-00	Control Enhancements:	SC-07(5).01-00	See Exhibit F			
			SC-07(6).01-00	Control Enhancements:	SC-07(6).01-00	See Exhibit F			
			SC-07(7).01-00	Control Enhancements:	SC-07(7).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(8).01-00	Control Enhancements:	SC-07(8).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(9).01-00	Control Enhancements:	SC-07(9).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(10).01-00	Control Enhancements:	SC-07(10).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(11).01-00	Control Enhancements:	SC-07(11).01-00	See Exhibit F			
			SC-07(12).01-00	Control Enhancements:	SC-07(12).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(13).01-00	Control Enhancements:	SC-07(13).01-00	See Exhibit F			
			SC-07(14).01-00	Control Enhancements:	SC-07(14).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(15).01-00	Control Enhancements:	SC-07(15).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(16).01-00	Control Enhancements:	SC-07(16).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(17).01-00	Control Enhancements:	SC-07(17).01-00	See Exhibit F			
					Enhanced Supplemental	See Exhibit F			
			SC-07(18).01-00	Control Enhancements:	SC-07(18).01-00	See Exhibit F			

					Enhanced Supplemental	See Exhibit F		
			SC-08.01-00	SC-8 TRANSMISSION INTEGRITY	SC-08.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-08(1).01-00	Control Enhancements:	SC-08(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-08(2).01-00	Control Enhancements:	SC-08(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-09.01-00	SC-9 TRANSMISSION CONFIDENTIALITY	SC-09.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-09(1).01-00	Control Enhancements:	SC-09(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-09(2).01-00		SC-09(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-10.01-00	SC-10 NETWORK DISCONNECT	SC-10.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-11.01-00	SC-11 TRUSTED PATH	SC-11.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-12.01-00	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND	SC-12.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			SC-12(1).01-00	Control Enhancements:	SC-12(1).01-00	See Exhibit F		
			SC-12(2).01-00	Control Enhancements:	SC-12(2).01-00	See Exhibit F		
			SC-12(3).01-00	Control Enhancements:	SC-12(3).01-00	See Exhibit F		
			SC-12(4).01-00	Control Enhancements:	SC-12(4).01-00	See Exhibit F		
			SC-12(5).01-00	Control Enhancements:	SC-12(5).01-00	See Exhibit F		
			SC-13.01-00	SC-13 USE OF CRYPTOGRAPHY	SC-13.01-00	See Exhibit F		
			SC-13(1).01-00	Control Enhancements:	SC-13(1).01-00	See Exhibit F		
			SC-13(2).01-00	Control Enhancements:	SC-13(2).01-00	See Exhibit F		
			SC-13(3).01-00	Control Enhancements:	SC-13(3).01-00	See Exhibit F		
			SC-13(4).01-00	Control Enhancements:	SC-13(4).01-00	See Exhibit F		
			SC-14.01-00	SC-14 PUBLIC ACCESS PROTECTIONS	SC-14.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-15.01-00	SC-15 COLLABORATIVE COMPUTING DEVICES	SC-15.01-00	See Exhibit F		
			SC-15.01-00		SC-15.01-00	See Exhibit F		

			SC-15.01-00		SC-15.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-15(1).01-00	Control Enhancements:	SC-15(1).01-00	See Exhibit F		
			SC-15(2).01-00	Control Enhancements:	SC-15(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-15(3).01-00	Control Enhancements:	SC-15(3).01-00	See Exhibit F		
			SC-16.01-00	SC-16 TRANSMISSION OF SECURITY ATTRIBUTES	SC-16.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			SC-16(1).01-00	Control Enhancements:	SC-16(1).01-00	See Exhibit F		
			SC-17.01-00	SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-18.01-00	SC-18 MOBILE CODE	SC-18.01-00	See Exhibit F		
			SC-18.01-01		SC-18.01-01	See Exhibit F		
			SC-18.01-02		SC-18.01-02	See Exhibit F		
			SC-18.01-03		SC-18.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-18(1).01-00	Control Enhancements:	SC-18(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-18(2).01-00		SC-18(2).01-00	See Exhibit F		
			SC-18(3).01-00		SC-18(3).01-00	See Exhibit F		
			SC-18(4).01-00		SC-18(4).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-19.01-00	SC-19 VOICE OVER INTERNET PROTOCOL	SC-19.01-00	See Exhibit F		
			SC-19.01-01		SC-19.01-01	See Exhibit F		
			SC-19.01-02		SC-19.01-02	See Exhibit F		
			SC-20.01-00	SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE	SC-20.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			SC-20(1).01-00	Control Enhancements:	SC-20(1).01-00	See Exhibit F		
						See Exhibit F		
						See Exhibit F		
			SC-21.01-00	SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE	SC-21.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		

						See Exhibit F		
			SC-21(1).01-00	Control Enhancements:	SC-21(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-22.01-00	SC-22 ARCHITECTURE AND PROVISIONING FOR NAME /	SC-22.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-23.01-00	SC-23 SESSION AUTHENTICITY	SC-23.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-23(1).01-00	Control Enhancements:	SC-23(1).01-00	See Exhibit F		
			SC-23(2).01-00	Control Enhancements:	SC-23(2).01-00	See Exhibit F		
			SC-23(3).01-00	Control Enhancements:	SC-23(3).01-00	See Exhibit F		
			SC-23(4).01-00	Control Enhancements:	SC-23(4).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-24.01-00	SC-24 FAIL IN KNOWN STATE	SC-24.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-25.01-00	SC-25 THIN NODES	SC-25.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-26.01-00	SC-26 HONEYPOTS	SC-26.01-00	See Exhibit F		
			SC-26(1).01-00		SC-26(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-27.01-00	SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS	SC-27.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-28.01-00	SC-28 PROTECTION OF INFORMATION AT REST	SC-28.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-28(1).01-00	Control Enhancements:	SC-28(1).01-00	See Exhibit F		
			SC-29.01-00	SC-29 HETEROGENEITY	SC-29.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-30.01-00	SC-30 VIRTUALIZATION TECHNIQUES	SC-30.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-30(1).01-00	Control Enhancements:	SC-30(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-30(2).01-00	Control Enhancements:	SC-30(2).01-00	See Exhibit F		
			SC-31.01-00	SC-31 COVERT CHANNEL ANALYSIS	SC-31.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-31(1).01-00	Control Enhancements:	SC-31(1).01-00	See Exhibit F		

			SC-32.01-00	SC-32 INFORMATION SYSTEM PARTITIONING	SC-32.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-33.01-00	SC-33 TRANSMISSION PREPARATION INTEGRITY	SC-33.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SC-34.01-00	SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS	SC-34.01-00	See Exhibit F		
			SC-34.01-01		SC-34.01-01	See Exhibit F		
			SC-34.01-02		SC-34.01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SC-34(1).01-00	Control Enhancements:	SC-34(1).01-00	See Exhibit F		
						See Exhibit F		
			SC-34(2).01-00	Control Enhancements:	SC-34(2).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
SI			SI-01.01-00	SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND	SI-01.01-00	See Exhibit F		
			SI-01.01-01		SI-01.01-01	See Exhibit F		
			SI-01.01-02		SI-01.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-02.01-00	SI-2 FLAW REMEDIATION	SI-02.01-00	See Exhibit F		
			SI-02.01-01		SI-02.01-01	See Exhibit F		
			SI-02.01-02		SI-02.01-02	See Exhibit F		
			SI-02.01-03		SI-02.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
						See Exhibit F		
			SI-02(1).01-00	Control Enhancements:	SI-02(1).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-02(2).01-00	Control Enhancements:	SI-02(2).01-00	See Exhibit F		
			SI-02(3).01-00	Control Enhancements:	SI-02(3).01-00	See Exhibit F		
			SI-02(4).01-00	Control Enhancements:	SI-02(4).01-00	See Exhibit F		
			SI-03.01-00	SI-3 MALICIOUS CODE PROTECTION	SI-03.01-00	See Exhibit F		
			SI-03.01-01		SI-03.01-01	See Exhibit F		
			SI-03.01-02		SI-03.01-02	See Exhibit F		
			SI-03.01-03		SI-03.01-03	See Exhibit F		
			SI-03.01-04		SI-03.01-04	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-03(1).01-00	Control Enhancements:	SI-03(1).01-00	See Exhibit F		

			SI-03(2).01-00	Control Enhancements:	SI-03(2).01-00	See Exhibit F		
			SI-03(3).01-00	Control Enhancements:	SI-03(3).01-00	See Exhibit F		
			SI-03(4).01-00	Control Enhancements:	SI-03(4).01-00	See Exhibit F		
			SI-03(5).01-00	Control Enhancements:	SI-03(5).01-00	See Exhibit F		
			SI-03(6).01-00	Control Enhancements:	SI-03(6).01-00	See Exhibit F		
			SI-04.01-00	SI-4 INFORMATION SYSTEM MONITORING	SI-04.01-00	See Exhibit F		
			SI-04.01-01		SI-04.01-01	See Exhibit F		
			SI-04.01-02		SI-04.01-02	See Exhibit F		
			SI-04.01-03		SI-04.01-03	See Exhibit F		
			SI-04.01-04		SI-04.01-04	See Exhibit F		
			SI-04.01-05		SI-04.01-05	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-04(1).01-00	Control Enhancements:	SI-04(1).01-00	See Exhibit F		
			SI-04(2).01-00	Control Enhancements:	SI-04(2).01-00	See Exhibit F		
			SI-04(3).01-00	Control Enhancements:	SI-04(3).01-00	See Exhibit F		
			SI-04(4).01-00	Control Enhancements:	SI-04(4).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-04(5).01-00	Control Enhancements:	SI-04(5).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-04(6).01-00	Control Enhancements:	SI-04(6).01-00	See Exhibit F		
			SI-04(7).01-00	Control Enhancements:	SI-04(7).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-04(8).01-00	Control Enhancements:	SI-04(8).01-00	See Exhibit F		
			SI-04(9).01-00	Control Enhancements:	SI-04(9).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-04(10).01-00	Control Enhancements:	SI-04(10).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-04(11).01-00	Control Enhancements:	SI-04(11).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-04(12).01-00	Control Enhancements:	SI-04(12).01-00	See Exhibit F		
			SI-04(13).01-00	Control Enhancements:	SI-04(13).01-00	See Exhibit F		
			SI-04(13).01-01	Control Enhancements:	SI-04(13).01-01	See Exhibit F		
			SI-04(13).01-02	Control Enhancements:	SI-04(13).01-02	See Exhibit F		
			SI-04(13).01-03	Control Enhancements:	SI-04(13).01-03	See Exhibit F		

			SI-04(14).01-00	Control Enhancements:	SI-04(14).01-00	See Exhibit F		
			SI-04(15).01-00	Control Enhancements:	SI-04(15).01-00	See Exhibit F		
			SI-04(16).01-00	Control Enhancements:	SI-04(16).01-00	See Exhibit F		
			SI-04(17).01-00	Control Enhancements:	SI-04(17).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-05.01-00	SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-05.01-00	See Exhibit F		
			SI-05.01-01		SI-05.01-01	See Exhibit F		
			SI-05.01-02		SI-05.01-02	See Exhibit F		
			SI-05.01-03		SI-05.01-03	See Exhibit F		
			SI-05.01-04		SI-05.01-04	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-05(1).01-00	Control Enhancements:	SI-05(1).01-00	See Exhibit F		
			SI-06.01-00	SI-6 SECURITY FUNCTIONALITY VERIFICATION	SI-06.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-06(1).01-00	Control Enhancements:	SI-06(1).01-00	See Exhibit F		
			SI-06(2).01-00	Control Enhancements:	SI-06(2).01-00	See Exhibit F		
			SI-06(3).01-00	Control Enhancements:	SI-06(3).01-00	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
			SI-07.01-00	SI-7 SOFTWARE AND INFORMATION INTEGRITY	SI-07.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-07(1).01-00	Control Enhancements:	SI-07(1).01-00	See Exhibit F		
			SI-07(2).01-00	Control Enhancements:	SI-07(2).01-00	See Exhibit F		
			SI-07(3).01-00	Control Enhancements:	SI-07(3).01-00	See Exhibit F		
			SI-07(4).01-00	Control Enhancements:	SI-07(4).01-00	See Exhibit F		
			SI-08.01-00	SI-8 SPAM PROTECTION	SI-08.01-00	See Exhibit F		
			SI-08.01-01		SI-08.01-01	See Exhibit F		
			SI-08.01-02		SI-08.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-08(1).01-00	Control Enhancements:	SI-08(1).01-00	See Exhibit F		
			SI-08(2).01-00	Control Enhancements:	SI-08(2).01-00	See Exhibit F		
			SI-09.01-00	SI-9 INFORMATION INPUT RESTRICTIONS	SI-09.01-00	See Exhibit F		
						See Exhibit F		
			SI-10.01-00	SI-10 INFORMATION INPUT VALIDATION	SI-10.01-00	See Exhibit F		
						See Exhibit F		

			SI-11.01-00	SI-11 ERROR HANDLING	SI-11.01-00	See Exhibit F		
			SI-11.01-01		SI-11.01-01	See Exhibit F		
			SI-11.01-02		SI-11.01-02	See Exhibit F		
			SI-11.01-03		SI-11.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-12.01-00	SI-12 INFORMATION OUTPUT HANDLING AND RETENTION	SI-12.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-13.01-00	SI-13 PREDICTABLE FAILURE PREVENTION	SI-13.01-00	See Exhibit F		
			SI-13.01-01		SI-13.01-01	See Exhibit F		
			SI-13.01-02		SI-13.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			SI-13(1).01-00	Control Enhancements:	SI-13(1).01-00	See Exhibit F		
			SI-13(2).01-00	Control Enhancements:	SI-13(2).01-00	See Exhibit F		
			SI-13(3).01-00	Control Enhancements:	SI-13(3).01-00	See Exhibit F		
			SI-13(4).01-00	Control Enhancements:	SI-13(4).01-00	See Exhibit F		
			SI-13(4).01-01	Control Enhancements:	SI-13(4).01-01	See Exhibit F		
			SI-13(4).01-02	Control Enhancements:	SI-13(4).01-02	See Exhibit F		
					Enhanced Supplemental	See Exhibit F		
PM			PM-01.01-00	PM-1 INFORMATION SECURITY PROGRAM PLAN	PM-01.01-00	See Exhibit F		
			PM-01.01-01		PM-01.01-01	See Exhibit F		
			PM-01.01-02		PM-01.01-02	See Exhibit F		
			PM-01.01-03		PM-01.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-02.01-00	PM-2 SENIOR INFORMATION SECURITY OFFICER	PM-02.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-03.01-00	PM-3 INFORMATION SECURITY RESOURCES	PM-03.01-00	See Exhibit F		
			PM-03.01-01		PM-03.01-01	See Exhibit F		
			PM-03.01-02		PM-03.01-02	See Exhibit F		
			PM-03.01-03		PM-03.01-03	See Exhibit F		
						See Exhibit F		
			PM-04.01-00	PM-4 PLAN OF ACTION AND MILESTONES PROCESS	PM-04.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-05.01-00	PM-5 INFORMATION SYSTEM INVENTORY	PM-05.01-00	See Exhibit F		

					Supplemental Guidance	See Exhibit F		
			PM-06.01-00	PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE	PM-06.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-07.01-00	PM-7 ENTERPRISE ARCHITECTURE	PM-07.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-08.01-00	PM-8 CRITICAL INFRASTRUCTURE PLAN	PM-08.01-00	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-09.01-00	PM-9 RISK MANAGEMENT STRATEGY	PM-09.01-00	See Exhibit F		
			PM-09.01-01		PM-09.01-01	See Exhibit F		
			PM-09.01-02		PM-09.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-10.01-00	PM-10 SECURITY AUTHORIZATION PROCESS	PM-10.01-00	See Exhibit F		
			PM-10.01-01		PM-10.01-01	See Exhibit F		
			PM-10.01-02		PM-10.01-02	See Exhibit F		
			PM-10.01-03		PM-10.01-03	See Exhibit F		
					Supplemental Guidance	See Exhibit F		
			PM-11.01-00	PM-11 MISSION/BUSINESS PROCESS DEFINITION	PM-11.01-00	See Exhibit F		
			PM-11.01-01		PM-11.01-01	See Exhibit F		
			PM-11.01-02		PM-11.01-02	See Exhibit F		
					Supplemental Guidance	See Exhibit F		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

HIPAA

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
HIPAA	00	0	HIPAA.00.0	CITATIONS	GENERAL RULES	Vendor will comply with all HIPAA GENERAL RULES			
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. (4) Ensure compliance with this subpart by its workforce.	Ensure CIA and protect against threats		
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. (iv) The probability and criticality of potential risks to electronic protected health information.	Reasonably consider factors in security compliance		
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.	Covered Entities CEs must comply with standards		
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 (2) Implement an equivalent alternative measure if reasonable and appropriate.	Required and Addressable Implementation Specification requirements		
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.	Ongoing review and modification of security measures		
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	P&P to manage security violations		
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.	Conduct vulnerability assessment		
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).	Implement security measures to reduce risk of security breaches		
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.	Worker sanction for P&P violations		
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.	Procedures to review system activity		
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.	Identify security official responsible for P&P		
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.	Implement P&P to ensure appropriate PHI access		
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.	Authorization/supervision for PHI access		
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.	Procedures to ensure appropriate PHI access		
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.	Procedures to terminate PHI access		
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.	P&P to authorize access to PHI		
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.	P&P to separate PHI from other operations		
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.	P&P to authorize access to PHI		

HIPAA	01	14	HIPAA.01.14	164.308(a)(4)(ii)(C)	Access Estabilshment 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.	P&P to grant access to PHI		
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).	Training program for workers and managers		
HIPAA	01	16	HIPAA.01.16	164.308(a)(5)(ii)(A)	Security Reminders	Vendor will distribute periodic security updates.	Distribute periodic security updates		
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.	Procedures to guard against malicious software		
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.	Procedures and monitoring of log-in attempts		
HIPAA	01	19	HIPAA.01.19	164.308(a)(5)(ii)(D)	Password Management	Vendor will have procedures for creating, changing, and safeguarding passwords.	Procedures for password management		
HIPAA	01	20	HIPAA.01.20	164.308(a)(6)(i)	**Security Incident Procedures**	Vendor will implement policies and procedures to address security incidents.	P&P to manage security incidents		
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.	Mitigate and document security incidents		
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.	Emergency response P&P		
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.	Data backup planning & procedures		
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.	Data recovery planning & procedures		
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.	Business continuity procedures		
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.	Contingency planning periodic testing procedures		
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.	Prioritize data and system criticality for contingency planning		
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.	Periodic security evaluation		
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.	CE implement BACs to ensure safeguards		
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).	Implement compliant BACs		
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.	P&P to limit access to systems and facilities		
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.	Procedures to support emergency operations and recovery		
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.	P&P to safeguard equipment and facilities		
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.	Facility access procedures for personnel		
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).	P&P to document security-related repairs and modifications		
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.	P&P to specify workstation environment & use		
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.	Physical safeguards for workstation access		
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.	P&P to govern receipt and removal of hardware and media		
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.	P&P to manage media and equipment disposal		
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.	P&P to remove PHI from media and equipment		
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.	Document hardware and media movement		
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.	Backup PHI before moving equipment		
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).	Technical (administrative) P&P to manage PHI access		
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.	Assign unique IDs to support tracking		
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.	Procedures to support emergency access		

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.	Session termination mechanisms		
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.	Mechanism for encryption of stored PHI		
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.	Procedures and mechanisms for monitoring system activity		
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.	P&P to safeguard PHI unauthorized alteration		
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.	Mechanisms to corroborate PHI not altered		
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.	Procedures to verify identities		
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.	Measures to guard against unauthorized access to transmitted PHI		
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.	Measures to ensure integrity of PHI on transmission		
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.	Mechanism for encryption of transmitted PHI		
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**	Hosting Provider will at all times comply with the terms of the Business Associate Agreement between CGI Technologies and Solutions Inc. and State of Vermont dated as of [December 13, 2012] (the "BAA"). (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.	CE must ensure BA safeguards PHI		
HIPAA	04	2	HIPAA.04.2	164.314(a)(2)	Business Associate Contracts	---	BACs must contain security language		
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.	Plan documents must reflect security safeguards		
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;	Plan sponsor to implement safeguards as appropriate		
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;	Security measures to separate PHI from plan sponsor and plan		
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	Ensure subcontractors safeguard PHI		
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.	Plan sponsors report breaches to health plan		
HIPAA	04	8	HIPAA.04.8	164.316(a)	**Policies and Procedures**	---	P&P to ensure safeguards to PHI		
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.	Document P&P and actions & activities		
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.	Retain documentation for 6 years		
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.	Documentation available to system administrators		
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.	Periodic review and updates to changing needs		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

PHI and Privacy

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
PHI	01	0	PHI.01.0	PHI and Privacy,		See Exhibit F		
PHI	01	1	PHI.01.1	PHI and Privacy,	Testing and Revision Procedures	See Exhibit F		
PHI	01	2	PHI.01.2	PHI and Privacy,	Encryption	See Exhibit F		
PHI	01	3	PHI.01.3	PHI and Privacy,		See Exhibit F		
PHI	01	4	PHI.01.4	PHI and Privacy, Access Control (§ 164.312(a)(1))	Data Backup and Storage	See Exhibit F		
PHI	01	5	PHI.01.5	PHI and Privacy, Access Control (§ 164.312(a)(1))		See Exhibit F		
PHI	01	6	PHI.01.6	PHI and Privacy, Access Control (§ 164.312(a)(1))	Unique User Identification	See Exhibit F		
PHI	01	7	PHI.01.7	PHI and Privacy, Access Control (§ 164.312(a)(1))	Emergency Access Procedure	See Exhibit F		
PHI	01	8	PHI.01.8	PHI and Privacy, Access Control (§ 164.312(a)(1))	Automatic Logoff	See Exhibit F		
PHI	01	9	PHI.01.9	PHI and Privacy, Assigned Security Responsibility (§ 164.308(a)(2))	Information System Activity Review	See Exhibit F		
PHI	01	10	PHI.01.10	PHI and Privacy, Audit Controls (§ 164.312(b))	Encryption and Decryption	See Exhibit F		
PHI	01	11	PHI.01.11	PHI and Privacy, Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))		See Exhibit F		
PHI	01	12	PHI.01.12	PHI and Privacy, Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))		See Exhibit F		
PHI	01	13	PHI.01.13	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))	Business Associate Contracts	See Exhibit F		
PHI	01	14	PHI.01.14	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))		See Exhibit F		
PHI	01	15	PHI.01.15	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))		See Exhibit F		
PHI	01	16	PHI.01.16	PHI and Privacy, Business Associate Contracts or Other Arrangements (§ 164.314(a)(2))		See Exhibit F		
PHI	01	17	PHI.01.17	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Response and Reporting	See Exhibit F		
PHI	01	18	PHI.01.18	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))		See Exhibit F		
PHI	01	19	PHI.01.19	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Data Backup Plan	See Exhibit F		
PHI	01	20	PHI.01.20	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Disaster Recovery Plan	See Exhibit F		
PHI	01	21	PHI.01.21	PHI and Privacy, Contingency Plan (§ 164.308(a)(7))	Emergency Model Operation Plan	See Exhibit F		
PHI	01	22	PHI.01.22	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))		See Exhibit F		
PHI	01	23	PHI.01.23	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))		See Exhibit F		
PHI	01	24	PHI.01.24	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))	Disposal	See Exhibit F		
PHI	01	25	PHI.01.25	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))	Media Reuse	See Exhibit F		

PHI	01	26	PHI.01.26	PHI and Privacy, Device and Media Controls (§ 164.310(d)(1))	Accountability	See Exhibit F		
PHI	01	27	PHI.01.27	PHI and Privacy, Evaluation (§ 164.308(a)(8))	Application and Data Criticality	See Exhibit F		
PHI	01	28	PHI.01.28	PHI and Privacy, Evaluation (§ 164.308(a)(8))		See Exhibit F		
PHI	01	29	PHI.01.29	PHI and Privacy, Evaluation (§ 164.308(a)(8))		See Exhibit F		
PHI	01	30	PHI.01.30	PHI and Privacy, Evaluation (§ 164.308(a)(8))	ISO 27002 Certificate of Conformance -	See Exhibit F		
PHI	01	31	PHI.01.31	PHI and Privacy, Evaluation (§ 164.308(a)(8))	ISO 27001 Certification	See Exhibit F		
PHI	01	32	PHI.01.32	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Written Contracts or other Arrangements	See Exhibit F		
PHI	01	33	PHI.01.33	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))		See Exhibit F		
PHI	01	34	PHI.01.34	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))		See Exhibit F		
PHI	01	35	PHI.01.35	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Facility Security Plan	See Exhibit F		
PHI	01	36	PHI.01.36	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Access Control and Validation Procedures	See Exhibit F		
PHI	01	37	PHI.01.37	PHI and Privacy, Facility Access Controls (§ 164.310(a)(1))	Maintenance Records	See Exhibit F		
PHI	01	38	PHI.01.38	PHI and Privacy, General Scope of Services		See Exhibit F		
PHI	01	39	PHI.01.39	PHI and Privacy, Information Access Management (§ 164.308(a)(4))	Termination Procedures	See Exhibit F		
PHI	01	40	PHI.01.40	PHI and Privacy, Information Access Management (§ 164.308(a)(4))		See Exhibit F		
PHI	01	41	PHI.01.41	PHI and Privacy, Information Access Management (§ 164.308(a)(4))	Isolating Health Care Clearinghouse Functions	See Exhibit F		
PHI	01	42	PHI.01.42	PHI and Privacy, Information Access Management (§ 164.308(a)(4))	Access Authorization	See Exhibit F		
PHI	01	43	PHI.01.43	PHI and Privacy, Integrity (§ 164.312(c)(1))		See Exhibit F		
PHI	01	44	PHI.01.44	PHI and Privacy, Notification in the Case of Breach of Unsecured PHI (§ 164.410)	ePHI Documentation Review	See Exhibit F		
PHI	01	45	PHI.01.45	PHI and Privacy, Notification in the Case of Breach of Unsecured PHI (§ 164.410)		See Exhibit F		
PHI	01	46	PHI.01.46	PHI and Privacy, Notification in the Case of Breach of Unsecured PHI (§ 164.410)	Timeliness of Notification	See Exhibit F		
PHI	01	47	PHI.01.47	PHI and Privacy, Person or Entity Authentication (§ 164.312(d))		See Exhibit F		
PHI	01	48	PHI.01.48	PHI and Privacy, Person or Entity Authentication (§ 164.312(d))	Mechanism to Authenticate ePHI	See Exhibit F		
PHI	01	49	PHI.01.49	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Policies and Procedures	See Exhibit F		

PHI	01	50	PHI.01.50	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Documentation	See Exhibit F		
PHI	01	51	PHI.01.51	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Time Limit	See Exhibit F		
PHI	01	52	PHI.01.52	PHI and Privacy, Policies and Procedures and Documentation Requirements (§ 164.316)	Documentation Availability	See Exhibit F		
PHI	01	53	PHI.01.53	PHI and Privacy, Privacy Requirements		See Exhibit F		
PHI	01	54	PHI.01.54	PHI and Privacy, Requirements for Group Health Plans (§ 164.314(b)(1))		See Exhibit F		
PHI	01	55	PHI.01.55	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))		See Exhibit F		
PHI	01	56	PHI.01.56	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))		See Exhibit F		
PHI	01	57	PHI.01.57	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))	Security Reminders	See Exhibit F		
PHI	01	58	PHI.01.58	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))	Protection from Malicious Software	See Exhibit F		
PHI	01	59	PHI.01.59	PHI and Privacy, Security Awareness and Training (§ 164.308(a)(5))	Login Monitoring	See Exhibit F		
PHI	01	60	PHI.01.60	PHI and Privacy, Security Incident Procedures (§ 164.308(a)(6))	Password Management	See Exhibit F		
PHI	01	61	PHI.01.61	PHI and Privacy, Security Incident Procedures (§ 164.308(a)(6))		See Exhibit F		
PHI	01	62	PHI.01.62	PHI and Privacy, Security Management Process (§ 164.308(a)(1))		See Exhibit F		
PHI	01	63	PHI.01.63	PHI and Privacy, Security Management Process (§ 164.308(a)(1))		See Exhibit F		
PHI	01	64	PHI.01.64	PHI and Privacy, Security Management Process (§ 164.308(a)(1))	Risk Analysis	See Exhibit F		
PHI	01	65	PHI.01.65	PHI and Privacy, Security Management Process (§ 164.308(a)(1))	Risk Management	See Exhibit F		
PHI	01	66	PHI.01.66	PHI and Privacy, Security Management Process (§ 164.308(a)(1))	Sanction Policy	See Exhibit F		
PHI	01	67	PHI.01.67	PHI and Privacy, Security Requirements		See Exhibit F		
PHI	01	68	PHI.01.68	PHI and Privacy, Transmission Security (§ 164.312(e)(1))		See Exhibit F		
PHI	01	69	PHI.01.69	PHI and Privacy, Transmission Security (§ 164.312(e)(1))		See Exhibit F		
PHI	01	70	PHI.01.70	PHI and Privacy, Transmission Security (§ 164.312(e)(1))	Integrity Controls	See Exhibit F		
PHI	01	71	PHI.01.71	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	72	PHI.01.72	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		

PHI	01	73	PHI.01.73	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	74	PHI.01.74	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	75	PHI.01.75	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	76	PHI.01.76	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	77	PHI.01.77	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	78	PHI.01.78	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	79	PHI.01.79	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	80	PHI.01.80	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	81	PHI.01.81	PHI and Privacy, Uses and Disclosures: Organizational requirements (§ 164.504 (e)(2))		See Exhibit F		
PHI	01	82	PHI.01.82	PHI and Privacy, Workforce Security (§ 164.308(a)(3))		See Exhibit F		
PHI	01	83	PHI.01.83	PHI and Privacy, Workforce Security (§ 164.308(a)(3))		See Exhibit F		
PHI	01	84	PHI.01.84	PHI and Privacy, Workforce Security (§ 164.308(a)(3))	Authorization and or Supervision	See Exhibit F		
PHI	01	85	PHI.01.85	PHI and Privacy, Workforce Security (§ 164.308(a)(3))	Workforce Clearance Procedures	See Exhibit F		
PHI	01	86	PHI.01.86	PHI and Privacy, Workstation Security (§ 164.310(c))		See Exhibit F		
PHI	01	87	PHI.01.87	PHI and Privacy, Workstation Use (§ 164.310(b))		See Exhibit F		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

IRS 1075

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
IRS	01	0	IRS.01.0	IRS 1075	Audit	The audit trail shall capture all successful login and logoff attempts.			
IRS	01	1	IRS.01.1	IRS 1075	Audit	The audit trail shall be protected from unauthorized access, use, deletion or modification.	Ensure CIA and protect against threats		
IRS	01	2	IRS.01.2	IRS 1075	Audit	The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.	Reasonably consider factors in security compliance		
IRS	01	3	IRS.01.3	IRS 1075	Audit	The audit trail shall capture all actions, connections and requests performed by privileged functions.	Covered Entities CEs must comply with standards		
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).	Required and Addressable Implementation Specification requirements		
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).	Ongoing review and modification of security measures		
IRS	01	6	IRS.01.6	IRS 1075	Audit	The audit trail shall capture all identification and authentication attempts.			
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.	P&P to manage security violations		
IRS	01	8	IRS.01.8	IRS 1075	Audit	The audit trail shall capture all unsuccessful login and authorization attempts.	Conduct vulnerability assessment		
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).	Implement security measures to reduce risk of security breaches		
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).	Worker sanction for P&P violations		
IRS	01	11	IRS.01.11	IRS 1075	Audit	The audit trail shall capture system startup and shutdown functions.	Procedures to review system activity		
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.	Identify security official responsible for P&P		
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.	Implement P&P to ensure appropriate PHI access		
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.	Authorization/supervision for PHI access		
IRS	01	15	IRS.01.15	IRS 1075	Audit	The audit trail shall capture the enabling or disabling of audit report generation services.	Procedures to ensure appropriate PHI access		
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.	Procedures to terminate PHI access		
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.	P&P to authorize access to PHI		
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)	P&P to separate PHI from other operations		
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.	P&P to authorize access to PHI		
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.	P&P to grant access to PHI		
IRS	01	21	IRS.01.21	IRS 1075	Password	User account lockout feature shall disable the user account after 3 unsuccessful login attempts.	Training program for workers and managers		
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.	Distribute periodic security updates		
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.	Procedures to guard against malicious software		
IRS	01	24	IRS.01.24	IRS 1075	Password	System initialization (boot) settings shall be password-protected.	Procedures and monitoring of log-in attempts		
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.	Procedures for password management		
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.	P&P to manage security incidents		
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.	Mitigate and document security incidents		
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.	Emergency response P&P		
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.	Data backup planning & procedures		
IRS	01	30	IRS.01.30	IRS 1075	Password	Password changes for standard and privileged users shall be systematically enforced where possible.	Data recovery planning & procedures		
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.	Business continuity procedures		
IRS	01	32	IRS.01.32	IRS 1075	Password	Default vendor passwords shall be changed upon successful installation of the information system product.	Contingency planning periodic testing procedures		
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.	Prioritize data and system criticality for contingency planning		
IRS	01	34	IRS.01.34	IRS 1075	Password	Account lockout duration shall be permanent until an authorized system administrator reinstates the user account.	Periodic security evaluation		
IRS	01	35	IRS.01.35	IRS 1075	General	The IRS Safeguards Report shall be correctly completed and requirements addressed if required	CE implement BACs to ensure safeguards		
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.			
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.	P&P to limit access to systems and facilities		

IRS	01	39	IRS.01.39	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment Technical Requirements	Hosting Provider will adhere to IRS 1075 Section 9.18.9 ,Web Portal: To utilize a web portal that provides FTI over the Internet to a customer,theagency must meet the following requirements:.The system architecture is configured as a three-tierarchitecture with physically separate systems that provide layered security of the FTI and access to the database through the application is limited.. 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.Access to FTI via the web portal requires a strong identity verification process. The authentication must use aminimum of two pieces of informational though more than two are recommended to verify the identity. One of the authentication elements must bea 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 asecure 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.	Procedures to support emergency operations and recovery		
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.	P&P to safeguard equipment and facilities		
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 Hosting Provider 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.	Facility access procedures for personnel		
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.	P&P to document security-related repairs and modifications		
IRS	01	43	IRS.01.43	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment Technical Requirements	—	P&P to specify workstation environment & use		
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.	Physical safeguards for workstation access		
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 Hosting Provider's network. This does not apply to the Hosting Provider's customers who access FTI through a customer service web portal. All Hosting Provider 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.	P&P to govern receipt and removal of hardware and media		
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.	P&P to manage media and equipment disposal		
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 Hosting Provider 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.	P&P to remove PHI from media and equipment		
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.	Document hardware and media movement		
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.	Backup PHI before moving equipment		

IRS	01	50	IRS.01.50	IRS 1075	Section 9.18.14 Protecting FTI in a Cloud Computing Environment - Technical Requirements	---			
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 Hosting Provider must have policies in place to restrict access to FTI to authorized users.	Assign unique IDs to support tracking		
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.	Procedures to support emergency access		
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.	Session termination mechanisms		
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.	Mechanism for encryption of stored PHI		
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.	Procedures and mechanisms for monitoring system activity		
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.	P&P to safeguard PHI unauthorized alteration		
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.	Mechanisms to corroborate PHI not altered		
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.	Procedures to verify identities		
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.	Measures to guard against unauthorized access to transmitted PHI		
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.	Measures to ensure integrity of PHI on transmission		
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 Hosting Provider must have compensating controls in place and properly applied which restrict access to VoIP traffic which contains FTI.			
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 Hosting Provider's network) the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode.	CE must ensure BA safeguards PHI		
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.	BACs must contain security language		
IRS	01	66	IRS.01.66	IRS 1075	Section 9.18.13 Protecting FTI in VOIP Networks - Technical Requirements	Each system within the Hosting Provider'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.	Plan documents must reflect security safeguards		
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.	Plan sponsor to implement safeguards as appropriate		

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.	Security measures to separate PHI from plan sponsor and plan		
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.	Ensure subcontractors safeguard PHI		
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.	Plan sponsors report breaches to health plan		
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).	P&P to ensure safeguards to PHI		
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.	Document P&P and actions & activities		
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.	Retain documentation for 6 years		
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:	Periodic review and updates to changing needs		
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.			
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			
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.			
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.			
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 Hosting Provider and, upon request, to the IRS reviewing office.			
IRS	01	82	IRS.01.82	IRS 1075	Contract Language	The Hosting Provider will have the right to void the contract if the contractor fails to provide the safeguards described above.			
IRS	01	81	IRS.01.81	IRS 1075		Hosting Provider must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the Hosting Provider's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches.			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

PCI-DSS

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
NA	NA	NA	NA	1	Remove sensitive authentication data and limit data retention.	See Exhibit F		
NA	NA	NA	NA	2	Protect the perimeter, internal, and wireless networks.	See Exhibit F		
NA	NA	NA	NA	3	Secure payment card applications.	See Exhibit F		
NA	NA	NA	NA	4	Monitor and control access to your systems.	See Exhibit F		
NA	NA	NA	NA	5	Protect stored cardholder data.	See Exhibit F		
NA	NA	NA	NA	6	Finalize remaining compliance efforts, and ensure all controls are in place.	See Exhibit F		
PCI	1	1	PCI.1.1	PCI-DSS	6	See Exhibit F		
PCI	1	1.1	PCI.1.1.1	PCI-DSS		See Exhibit F		
PCI	1	1.2	PCI.1.1.2	PCI-DSS	1	See Exhibit F		
PCI	1	1.3	PCI.1.1.3	PCI-DSS	2	See Exhibit F		
PCI	1	1.4	PCI.1.1.4	PCI-DSS	6	See Exhibit F		
PCI	1	1.5	PCI.1.1.5	PCI-DSS	2	See Exhibit F		
PCI	1	1.6	PCI.1.1.6	PCI-DSS	6	See Exhibit F		
PCI	1	2	PCI.1.2	PCI-DSS	2	See Exhibit F		
PCI	1	2.1	PCI.1.2.1	PCI-DSS		See Exhibit F		
PCI	1	2.2	PCI.1.2.2	PCI-DSS	2	See Exhibit F		
PCI	1	2.3	PCI.1.2.3	PCI-DSS	2	See Exhibit F		
PCI	1	3	PCI.1.3	PCI-DSS	2	See Exhibit F		
PCI	1	3.1	PCI.1.3.1	PCI-DSS		See Exhibit F		
PCI	1	3.2	PCI.1.3.2	PCI-DSS	2	See Exhibit F		
PCI	1	3.3	PCI.1.3.3	PCI-DSS	2	See Exhibit F		
PCI	1	3.4	PCI.1.3.4	PCI-DSS	2	See Exhibit F		
PCI	1	3.5	PCI.1.3.5	PCI-DSS	2	See Exhibit F		
PCI	1	3.6	PCI.1.3.6	PCI-DSS	2	See Exhibit F		
PCI	1	3.7	PCI.1.3.7	PCI-DSS	2	See Exhibit F		
PCI	1	3.8	PCI.1.3.8	PCI-DSS	2	See Exhibit F		
PCI	1	4	PCI.1.4	PCI-DSS	2	See Exhibit F		
PCI	2	0	PCI.2.0	PCI-DSS		See Exhibit F		
PCI	2	1	PCI.2.1	PCI-DSS	2	See Exhibit F		
PCI	2	1.1	PCI.2.1.1	PCI-DSS	2	See Exhibit F		
PCI	2	2	PCI.2.2	PCI-DSS	3	See Exhibit F		
PCI	2	2.1	PCI.2.2.1	PCI-DSS	3	See Exhibit F		
PCI	2	2.2	PCI.2.2.2	PCI-DSS	3	See Exhibit F		
PCI	2	2.3	PCI.2.2.3	PCI-DSS	3	See Exhibit F		
PCI	2	2.4	PCI.2.2.4	PCI-DSS	3	See Exhibit F		
PCI	2	3	PCI.2.3	PCI-DSS	2	See Exhibit F		
PCI	2	4	PCI.2.4	PCI-DSS	3	See Exhibit F		
PCI	3	0	PCI.3.0	PCI-DSS		See Exhibit F		
PCI	3	1	PCI.3.1	PCI-DSS	1	See Exhibit F		
PCI	3	1.1	PCI.3.1.1	PCI-DSS	1	See Exhibit F		

PCI	3	2	PCI.3.2	PCI-DSS	1	See Exhibit F		
PCI	3	2.1	PCI.3.2.1	PCI-DSS	1	See Exhibit F		
PCI	3	2.2	PCI.3.2.2	PCI-DSS	1	See Exhibit F		
PCI	3	2.3	PCI.3.2.3	PCI-DSS	1	See Exhibit F		
PCI	3	3	PCI.3.3	PCI-DSS	5	See Exhibit F		
PCI	3	4	PCI.3.4	PCI-DSS	5	See Exhibit F		
PCI	3	4.1	PCI.3.4.1	PCI-DSS	5	See Exhibit F		
PCI	3	5	PCI.3.5	PCI-DSS	5	See Exhibit F		
PCI	3	5.1	PCI.3.5.1	PCI-DSS	5	See Exhibit F		
PCI	3	5.2	PCI.3.5.2	PCI-DSS	5	See Exhibit F		
PCI	3	6	PCI.3.6	PCI-DSS	5	See Exhibit F		
PCI	3	6.1	PCI.3.6.1	PCI-DSS	5	See Exhibit F		
PCI	3	6.2	PCI.3.6.2	PCI-DSS	5	See Exhibit F		
PCI	3	6.3	PCI.3.6.3	PCI-DSS	5	See Exhibit F		
PCI	3	6.4	PCI.3.6.4	PCI-DSS	5	See Exhibit F		
PCI	3	6.5	PCI.3.6.5	PCI-DSS	5	See Exhibit F		
PCI	3	6.6	PCI.3.6.6	PCI-DSS	5	See Exhibit F		
PCI	3	6.7	PCI.3.6.7	PCI-DSS	5	See Exhibit F		
PCI	3	6.8	PCI.3.6.8	PCI-DSS	5	See Exhibit F		
PCI	4	0	PCI.4.0	PCI-DSS		See Exhibit F		
PCI	4	1	PCI.4.1	PCI-DSS	2	See Exhibit F		
PCI	4	1.1	PCI.4.1.1	PCI-DSS	2	See Exhibit F		
PCI	4	2	PCI.4.2	PCI-DSS	2	See Exhibit F		
PCI	5	0	PCI.5.0	PCI-DSS		See Exhibit F		
PCI	5	1	PCI.5.1	PCI-DSS	2	See Exhibit F		
PCI	5	1.1	PCI.5.1.1	PCI-DSS	2	See Exhibit F		
PCI	5	2	PCI.5.2	PCI-DSS	2	See Exhibit F		
PCI	6	0	PCI.6.0	PCI-DSS		See Exhibit F		
PCI	6	1	PCI.6.1	PCI-DSS	3	See Exhibit F		
PCI	6	2	PCI.6.2	PCI-DSS	3	See Exhibit F		
PCI	6	3	PCI.6.3	PCI-DSS	3	See Exhibit F		
PCI	6	3.1	PCI.6.3.1	PCI-DSS	3	See Exhibit F		
PCI	6	3.2	PCI.6.3.2	PCI-DSS	3	See Exhibit F		
PCI	6	4	PCI.6.4	PCI-DSS	3	See Exhibit F		
PCI	6	4.1	PCI.6.4.1	PCI-DSS	3	See Exhibit F		
PCI	6	4.2	PCI.6.4.2	PCI-DSS	3	See Exhibit F		
PCI	6	4.3	PCI.6.4.3	PCI-DSS	3	See Exhibit F		
PCI	6	4.4	PCI.6.4.4	PCI-DSS	3	See Exhibit F		
PCI	6	4.5	PCI.6.4.5	PCI-DSS	6	See Exhibit F		
PCI	6	4.5.1	PCI.6.4.5.1	PCI-DSS	6	See Exhibit F		
PCI	6	4.5.2	PCI.6.4.5.2	PCI-DSS	6	See Exhibit F		
PCI	6	4.5.3	PCI.6.4.5.3	PCI-DSS	6	See Exhibit F		
PCI	6	4.5.4	PCI.6.4.5.4	PCI-DSS	6	See Exhibit F		
PCI	6	5	PCI.6.5	PCI-DSS	3	See Exhibit F		
PCI	6	5.1	PCI.6.5.1	PCI-DSS	3	See Exhibit F		
PCI	6	5.2	PCI.6.5.2	PCI-DSS	3	See Exhibit F		

PCI	6	5.3	PCI.6.5.3	PCI-DSS	3	See Exhibit F		
PCI	6	5.4	PCI.6.5.4	PCI-DSS	3	See Exhibit F		
PCI	6	5.5	PCI.6.5.5	PCI-DSS	3	See Exhibit F		
PCI	6	5.6	PCI.6.5.6	PCI-DSS	3	See Exhibit F		
PCI	6	5.7	PCI.6.5.7	PCI-DSS	3	See Exhibit F		
PCI	6	5.8	PCI.6.5.8	PCI-DSS	3	See Exhibit F		
PCI	6	5.9	PCI.6.5.9	PCI-DSS	3	See Exhibit F		
PCI	6	6	PCI.6.6	PCI-DSS	3	See Exhibit F		
PCI	7	0	PCI.7.0	PCI-DSS		See Exhibit F		
PCI	7	1	PCI.7.1	PCI-DSS	4	See Exhibit F		
PCI	7	1.1	PCI.7.1.1	PCI-DSS	4	See Exhibit F		
PCI	7	1.2	PCI.7.1.2	PCI-DSS	4	See Exhibit F		
PCI	7	1.3	PCI.7.1.3	PCI-DSS	4	See Exhibit F		
PCI	7	1.4	PCI.7.1.4	PCI-DSS	4	See Exhibit F		
PCI	7	2	PCI.7.2	PCI-DSS	4	See Exhibit F		
PCI	7	2.1	PCI.7.2.1	PCI-DSS	4	See Exhibit F		
PCI	7	2.2	PCI.7.2.2	PCI-DSS	4	See Exhibit F		
PCI	7	2.3	PCI.7.2.3	PCI-DSS	4	See Exhibit F		
PCI	8	0	PCI.8.0	PCI-DSS		See Exhibit F		
PCI	8	1	PCI.8.1	PCI-DSS	4	See Exhibit F		
PCI	8	2	PCI.8.2	PCI-DSS	4	See Exhibit F		
PCI	8	3	PCI.8.3	PCI-DSS	4	See Exhibit F		
PCI	8	4	PCI.8.4	PCI-DSS	4	See Exhibit F		
PCI	8	5	PCI.8.5	PCI-DSS	4	See Exhibit F		
PCI	8	5.1	PCI.8.5.1	PCI-DSS	4	See Exhibit F		
PCI	8	5.2	PCI.8.5.2	PCI-DSS	4	See Exhibit F		
PCI	8	5.3	PCI.8.5.3	PCI-DSS	4	See Exhibit F		
PCI	8	5.4	PCI.8.5.4	PCI-DSS	4	See Exhibit F		
PCI	8	5.5	PCI.8.5.5	PCI-DSS	4	See Exhibit F		
PCI	8	5.6	PCI.8.5.6	PCI-DSS	4	See Exhibit F		
PCI	8	5.7	PCI.8.5.7	PCI-DSS	4	See Exhibit F		
PCI	8	5.8	PCI.8.5.8	PCI-DSS	4	See Exhibit F		
PCI	8	5.9	PCI.8.5.9	PCI-DSS	4	See Exhibit F		
PCI	8	5.10	PCI.8.5.10	PCI-DSS	4	See Exhibit F		
PCI	8	5.11	PCI.8.5.11	PCI-DSS	4	See Exhibit F		
PCI	8	5.12	PCI.8.5.12	PCI-DSS	4	See Exhibit F		
PCI	8	5.13	PCI.8.5.13	PCI-DSS	4	See Exhibit F		
PCI	8	5.14	PCI.8.5.14	PCI-DSS	4	See Exhibit F		
PCI	8	5.15	PCI.8.5.15	PCI-DSS	4	See Exhibit F		
PCI	8	5.16	PCI.8.5.16	PCI-DSS	4	See Exhibit F		
PCI	9	0	PCI.9.0	PCI-DSS		See Exhibit F		
PCI	9	1	PCI.9.1	PCI-DSS	2	See Exhibit F		
PCI	9	1.1	PCI.9.1.1	PCI-DSS	2	See Exhibit F		
PCI	9	1.2	PCI.9.1.2	PCI-DSS	2	See Exhibit F		
PCI	9	1.3	PCI.9.1.3	PCI-DSS	2	See Exhibit F		
PCI	9	2	PCI.9.2	PCI-DSS	5	See Exhibit F		

PCI	9	3	PCI.9.3	PCI-DSS	5	See Exhibit F		
PCI	9	3.1	PCI.9.3.1	PCI-DSS	5	See Exhibit F		
PCI	9	3.2	PCI.9.3.2	PCI-DSS	5	See Exhibit F		
PCI	9	3.3	PCI.9.3.3	PCI-DSS	5	See Exhibit F		
PCI	9	4	PCI.9.4	PCI-DSS	5	See Exhibit F		
PCI	9	5	PCI.9.5	PCI-DSS	5	See Exhibit F		
PCI	9	6	PCI.9.6	PCI-DSS	5	See Exhibit F		
PCI	9	7	PCI.9.7	PCI-DSS	5	See Exhibit F		
PCI	9	7.1	PCI.9.7.1	PCI-DSS	5	See Exhibit F		
PCI	9	7.2	PCI.9.7.2	PCI-DSS	5	See Exhibit F		
PCI	9	8	PCI.9.8	PCI-DSS	5	See Exhibit F		
PCI	9	9	PCI.9.9	PCI-DSS	5	See Exhibit F		
PCI	9	9.1	PCI.9.9.1	PCI-DSS	5	See Exhibit F		
PCI	9	10	PCI.9.10	PCI-DSS	1	See Exhibit F		
PCI	9	10.1	PCI.9.10.1	PCI-DSS	1	See Exhibit F		
PCI	9	10.2	PCI.9.10.2	PCI-DSS	1	See Exhibit F		
PCI	10	0	PCI.10.0	PCI-DSS		See Exhibit F		
PCI	10	1	PCI.10.1	PCI-DSS	4	See Exhibit F		
PCI	10	2	PCI.10.2	PCI-DSS	4	See Exhibit F		
PCI	10	2.1	PCI.10.2.1	PCI-DSS	4	See Exhibit F		
PCI	10	2.2	PCI.10.2.2	PCI-DSS	4	See Exhibit F		
PCI	10	2.3	PCI.10.2.3	PCI-DSS	4	See Exhibit F		
PCI	10	2.4	PCI.10.2.4	PCI-DSS	4	See Exhibit F		
PCI	10	2.5	PCI.10.2.5	PCI-DSS	4	See Exhibit F		
PCI	10	2.6	PCI.10.2.6	PCI-DSS	4	See Exhibit F		
PCI	10	2.7	PCI.10.2.7	PCI-DSS	4	See Exhibit F		
PCI	10	3	PCI.10.3	PCI-DSS	4	See Exhibit F		
PCI	10	3.1	PCI.10.3.1	PCI-DSS	4	See Exhibit F		
PCI	10	3.2	PCI.10.3.2	PCI-DSS	4	See Exhibit F		
PCI	10	3.3	PCI.10.3.3	PCI-DSS	4	See Exhibit F		
PCI	10	3.4	PCI.10.3.4	PCI-DSS	4	See Exhibit F		
PCI	10	3.5	PCI.10.3.5	PCI-DSS	4	See Exhibit F		
PCI	10	3.6	PCI.10.3.6	PCI-DSS	4	See Exhibit F		
PCI	10	4	PCI.10.4	PCI-DSS	4	See Exhibit F		
PCI	10	4.1	PCI.10.4.1	PCI-DSS	4	See Exhibit F		
PCI	10	4.2	PCI.10.4.2	PCI-DSS	4	See Exhibit F		
PCI	10	4.3	PCI.10.4.3	PCI-DSS	4	See Exhibit F		
PCI	10	5	PCI.10.5	PCI-DSS	4	See Exhibit F		
PCI	10	5.1	PCI.10.5.1	PCI-DSS	4	See Exhibit F		
PCI	10	5.2	PCI.10.5.2	PCI-DSS	4	See Exhibit F		
PCI	10	5.3	PCI.10.5.3	PCI-DSS	4	See Exhibit F		
PCI	10	5.4	PCI.10.5.4	PCI-DSS	4	See Exhibit F		
PCI	10	5.5	PCI.10.5.5	PCI-DSS	4	See Exhibit F		
PCI	10	6	PCI.10.6	PCI-DSS	4	See Exhibit F		
PCI	10	7	PCI.10.7	PCI-DSS	4	See Exhibit F		
PCI	11	0	PCI.11.0	PCI-DSS		See Exhibit F		

PCI	11	1	PCI.11.1	PCI-DSS	4	See Exhibit F		
PCI	11	2	PCI.11.2	PCI-DSS	2	See Exhibit F		
PCI	11	2.1	PCI.11.2.1	PCI-DSS	2	See Exhibit F		
PCI	11	2.2	PCI.11.2.2	PCI-DSS	2	See Exhibit F		
PCI	11	2.3	PCI.11.2.3	PCI-DSS	2	See Exhibit F		
PCI	11	3	PCI.11.3	PCI-DSS	2	See Exhibit F		
PCI	11	3.1	PCI.11.3.1	PCI-DSS	2	See Exhibit F		
PCI	11	3.2	PCI.11.3.2	PCI-DSS	2	See Exhibit F		
PCI	11	4	PCI.11.4	PCI-DSS	2	See Exhibit F		
PCI	11	5	PCI.11.5	PCI-DSS	4	See Exhibit F		
PCI	12	0	PCI.12.0	PCI-DSS		See Exhibit F		
PCI	12	1	PCI.12.1	PCI-DSS	6	See Exhibit F		
PCI	12	1.1	PCI.12.1.1	PCI-DSS	6	See Exhibit F		
PCI	12	1.2	PCI.12.1.2	PCI-DSS	1	See Exhibit F		
PCI	12	1.3	PCI.12.1.3	PCI-DSS	6	See Exhibit F		
PCI	12	2	PCI.12.2	PCI-DSS	6	See Exhibit F		
PCI	12	3	PCI.12.3	PCI-DSS	6	See Exhibit F		
PCI	12	3.1	PCI.12.3.1	PCI-DSS	6	See Exhibit F		
PCI	12	3.2	PCI.12.3.2	PCI-DSS	6	See Exhibit F		
PCI	12	3.3	PCI.12.3.3	PCI-DSS	6	See Exhibit F		
PCI	12	3.4	PCI.12.3.4	PCI-DSS	6	See Exhibit F		
PCI	12	3.5	PCI.12.3.5	PCI-DSS	6	See Exhibit F		
PCI	12	3.6	PCI.12.3.6	PCI-DSS	6	See Exhibit F		
PCI	12	3.7	PCI.12.3.7	PCI-DSS	6	See Exhibit F		
PCI	12	3.8	PCI.12.3.8	PCI-DSS	6	See Exhibit F		
PCI	12	3.9	PCI.12.3.9	PCI-DSS	6	See Exhibit F		
PCI	12	3.10	PCI.12.3.10	PCI-DSS	6	See Exhibit F		
PCI	12	4	PCI.12.4	PCI-DSS	6	See Exhibit F		
PCI	12	5	PCI.12.5	PCI-DSS	6	See Exhibit F		
PCI	12	5.1	PCI.12.5.1	PCI-DSS	6	See Exhibit F		
PCI	12	5.2	PCI.12.5.2	PCI-DSS	6	See Exhibit F		
PCI	12	5.3	PCI.12.5.3	PCI-DSS	4	See Exhibit F		
PCI	12	5.4	PCI.12.5.4	PCI-DSS	6	See Exhibit F		
PCI	12	5.5	PCI.12.5.5	PCI-DSS	6	See Exhibit F		
PCI	12	6	PCI.12.6	PCI-DSS	6	See Exhibit F		
PCI	12	6.1	PCI.12.6.1	PCI-DSS	6	See Exhibit F		
PCI	12	6.2	PCI.12.6.2	PCI-DSS	6	See Exhibit F		
PCI	12	7	PCI.12.7	PCI-DSS	6	See Exhibit F		
PCI	12	8	PCI.12.8	PCI-DSS	2	See Exhibit F		
PCI	12	8.1	PCI.12.8.1	PCI-DSS	2	See Exhibit F		
PCI	12	8.2	PCI.12.8.2	PCI-DSS	2	See Exhibit F		
PCI	12	8.3	PCI.12.8.3	PCI-DSS	2	See Exhibit F		
PCI	12	8.4	PCI.12.8.4	PCI-DSS	2	See Exhibit F		
PCI	12	9	PCI.12.9	PCI-DSS	4	See Exhibit F		
PCI	12	9.1	PCI.12.9.1	PCI-DSS	4	See Exhibit F		
PCI	12	9.2	PCI.12.9.2	PCI-DSS	4	See Exhibit F		

PCI	12	9.3	PCI.12.9.3	PCI-DSS	4	See Exhibit F		
PCI	12	9.4	PCI.12.9.4	PCI-DSS	4	See Exhibit F		
PCI	12	9.5	PCI.12.9.5	PCI-DSS	4	See Exhibit F		
PCI	1	9.6	PCI.1.9.6	PCI-DSS	4	See Exhibit F		
PCI	A	1	PCI.A.1	PCI-DSS	3	See Exhibit F		
PCI	A	1.1	PCI.A.1.1	PCI-DSS	3	See Exhibit F		
PCI	A	1.2	PCI.A.1.2	PCI-DSS	3	See Exhibit F		
PCI	A	1.3	PCI.A.1.3	PCI-DSS	3	See Exhibit F		
PCI	A	1.4	PCI.A.1.4	PCI-DSS	3	See Exhibit F		

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

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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.		
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.		
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)		
SLN1	1	4	SLN1.1.4	SOA General		Solutions shall provide the ability to distribute services amongst different components and tiers of the architecture.		
SLN1	1	5	SLN1.1.5	SOA General		Solutions shall develop/integrate services using standardized Web Services formats.		
SLN1	1	6	SLN1.1.6	SOA General		Solutions shall allow for centralized service maintenance (new, update, delete).		
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.		
SLN1	1	8	SLN1.1.8	SOA General		Solutions shall ensure enterprise-wide access to services through all required channels.		
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.		
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).		
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.		
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		
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		
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		
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		
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.		
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		
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		
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.		
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		
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 (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.		
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		
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.		
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		
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		
SLN1	1	27	SLN1.1.27	Service Ownership		All services shall have key stakeholder/owners identified		
SLN1	1	28	SLN1.1.28	WSDL Development Standards		All WSDLs developed for Vermont shall conform to the WSDL Development Standards		
SLN1	1	29	SLN1.1.29	XSD Standardization		All SOA-related messages shall be formally defined with XSD (preferable) or DTDs.		
SLN1	1	30	SLN1.1.30	SOA Service Language		SOA-related services hosted should be implemented in Java.		
SLN1	1	31	SLN1.1.31	SOA policy		Implemented services shall rely on WS-Policy configurations for message reliability (WS-ReliableMessaging)		
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)		
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.		
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.		
SLN1	1	35	SLN1.1.35	SOA IdM Integration		SOA technology components shall rely on the central IdM technology components for authentication/authorization		
SLN1	1	36	SLN1.1.36	SOA Rules Integration		Business rules implemented with the rules engine should be accessed through a SOA service		
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.		
SLN1	1	38	SLN1.1.38	SOA General		Solutions shall provide reliable, once-only delivery of messages (guarantee of reliable and non-repetitive delivery).		
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 (including Electornic 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		
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.		
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		
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		
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		

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		
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		
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.		
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.		
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. (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.		
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.		
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.		
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).		
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.		
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.		
SLN1	1	56	SLN1.1.56	SOA General		Solutions shall support individual and group teamwork at design time and runtime.		
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.		
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.		
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.		
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.		

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.		
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]).		
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.		
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).		
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		
SLN1	1	66	SLN1.1.66	SOA General		A Service Registry shall serve as an integration point for runtime tooling		
SLN1	1	67	SLN1.1.67	SOA General		Service Bus shall subscribe to new or modified assets		
SLN1	1	68	SLN1.1.68	SOA General		Composite applications shall discover updated endpoints and WSDL locations		
SLN1	1	69	SLN1.1.69	SOA General		Runtime monitoring tooling shall publish metrics to the Service Registry		
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)		
SLN1	1	71	SLN1.1.71	SOA General		Shall provide dynamic discovery and service level monitoring of all artifacts deployed in the Application Server		
SLN1	1	72	SLN1.1.72	SOA General		Supplier 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		
SLN1	1	73	SLN1.1.73	SOA General		These SOA guildelines 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.		

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

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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		
SLN2	1	2	SLN2.1.2	Audit General		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.		
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.		
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.		
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.		
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.		
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		
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).		
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.		
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.		
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.		
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.		
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.	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.	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).	Auditing	
SLN2	1	17	SLN2.1.17	Audit General		Provide and retain transaction logs in accordance with the Harmonized Security and Privacy Framework.	Auditing	
SLN2	1	18	SLN2.1.18	Audit General		Provide reporting for security audits and compliance activities based on designated timeframes.	Auditing	
SLN2	1	19	SLN2.1.19	Audit General		Provide ability to set security controls for audit logs via role based access controls.	Auditing	
SLN2	1	20	SLN2.1.20	Audit General		Provide flexible audit report function (including on demand feature) and audit logging ability.	Auditing	
SLN2	1	21	SLN2.1.21	Audit General		Provide ability to perform the database capabilities to facilitate audit.	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.	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.	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).	Auditing	

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

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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.		
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.		
SLN3	1	3	SLN3.1.3	Business Intelligence General		Shared Analytics Infrastructure Solutions shall capture and load data via Service Oriented Architecture (SOA)-based services and the ability to schedule data integration and load jobs.		
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.		
SLN3	1	5	SLN3.1.5	Business Intelligence General		Shared Analytics Infrastructure Solutions shall create custom transformations and the ability to group and reuse mapping and transformation operations.		
SLN3	1	6	SLN3.1.6	Business Intelligence General		Solutions shall support multi-dimensional views and multidimensional tables.		
SLN3	1	7	SLN3.1.7	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support physical creation and storage of views as well as logical view.		
SLN3	1	8	SLN3.1.8	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support design to facilitate a single view of business data.		
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.		
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.		
SLN3	1	11	SLN3.1.11	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support data mining functions.		
SLN3	1	12	SLN3.1.12	Business Intelligence General		Shared Analytics Infrastructure Solutions shall 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.		
SLN3	1	14	SLN3.1.14	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support fast large volume data loading and shall capture real-time data.		
SLN3	1	15	SLN3.1.15	Business Intelligence General		Solutions shall impose graduated access to reports based on user role and agency requirements/permissions to better analyze program data.		
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.		
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.		
SLN3	1	18	SLN3.1.18	Business Intelligence General		Solutions shall be extensible and have a scalable data architecture incorporating State and external data.		
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).		
SLN3	1	20	SLN3.1.20	Business Intelligence General		Solutions shall provide the ability for user to create and customize reports, queries, and dashboards.		
SLN3	1	21	SLN3.1.21	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide comprehensive metadata management from source to target.		
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.		
SLN3	1	23	SLN3.1.23	Business Intelligence General		Shared Analytics Infrastructure Solutions shall import metadata from tools and data sources.		
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.		
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.		
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).		

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.		
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.		
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.		
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.		
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.		
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.		
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).		
SLN3	1	36	SLN3.1.36	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide scalable architecture.		
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.		
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, within the designed storage limits.		
SLN3	1	39	SLN3.1.39	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support scaling across regions.		
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.		
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.		
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).		
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		
SLN3	1	45	SLN3.1.45	Business Intelligence General		Shared Analytics Infrastructure Solutions shall provide workflow and collaboration support for administrator tasks.		
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)		
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.		
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]).		
SLN3	1	49	SLN3.1.49	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support various database connectivity (e.g. ODBC, JDBC).		
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).		
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		
SLN3	1	52	SLN3.1.52	Business Intelligence General		Shared Analytics Infrastructure Solutions shall support triggers, stored procedures and extension.		
SLN3	1	53	SLN3.1.53	Business Intelligence General		The Solution must allow the user to export formatted reports from the system in industry standard formats, e.g., Word, Excel, PDF, OF, etc.		
SLN3	1	54	SLN3.1.54	Business Intelligence General		Shared Analytics Infrastructure Solutions shall import metadata from tools and data sources.		
SLN3	1	55	SLN3.1.55	Business Intelligence General		The Solution must limit report views based on user security / access rights.		
SLN3	1	56	SLN3.1.56	Business Intelligence General		The Solution must notify and distribute reports based on user specified criteria.		
SLN3	1	57	SLN3.1.57	Business Intelligence General		The Solution must organize reports into a shared list (library).		
SLN3	1	58	SLN3.1.58	Business Intelligence General		The Solution must present data in graphical or chart format.		
SLN3	1	59	SLN3.1.59	Business Intelligence General		The Solution must roll-up (summarize data) and drill-down (view details) in reports online.		

SLN3	1	60	SLN3.1.60	Business Intelligence General		The Solution must schedule the generation of reports at specific times.		
SLN3	1	61	SLN3.1.61	Business Intelligence General		The Solution must sort data within reports in multiple ways.		
SLN3	1	62	SLN3.1.62	Business Intelligence General		The Solution must transmit reports to various designated recipients in a secure manner.		
SLN3	1	63	SLN3.1.63	Business Intelligence General		The Solution must restrict access to the shared list (library) or items within a shared list (library) to designated users.		
SLN3	1	64	SLN3.1.64	Business Intelligence General		The Solution shall generate ad-hoc and standard reports in real time as well as historical for incoming and outgoing contacts.		
SLN3	1	65	SLN3.1.65	Business Intelligence General		The Solution shall collect data and generate periodic reports as required by the Affordable Care Act.		
SLN3	1	66	SLN3.1.66	Business Intelligence General		The Solution shall develop and implement reports, dashboards, scorecards, predictive analytics, what-if analysis and statistical analysis.		
SLN3	1	67	SLN3.1.67	Business Intelligence General		The Solution shall generate reports necessary for the Health Insurance Exchange Entities, State and Federal officials, employers and other entities, such as insurance carriers.		
SLN3	1	68	SLN3.1.68	Business Intelligence General		The Solution shall Provide access to standardized reporting, ad hoc queries, and data visualization.		
SLN3	1	69	SLN3.1.69	Business Intelligence General		The Solution shall provide reports to users in online and offline formats, such as web, fax, and paper.		

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Master Data Management and Integration

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	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		—		
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 transformations		
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				
SLN4	1	73	SLN4.1.73	MDM & Integration				
SLN4	1	74	SLN4.1.74	MDM & Integration				
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	Notes	Evidence
SLN5	1	1	SLN5 1.1	Interface General							
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			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	Uni-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 (Carriers) 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 Tool) 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	CM	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		ID Management Interface	IdM	Bi-Directional	HBE		
SLN5	1	116	SLN51.116	Physical Interface		Scanning and paper processing interface	Scanning/Paper	Uni-Directional	HBE		
SLN5	1	117	SLN51.117	Physical Interface		Peoplesoft Interface	PS	Bi-Directional	HBE		

SLNS		1	118	SLNS1.118	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	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 ensure 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	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 - itegration/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.		
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	Notes	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	Specifics	Requirement Description	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 sender.		
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	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
SLN10	1	1	SLN10.1.1	DBMS		The RDBMS 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 RDBMS shall have the ability to optimize performance in transaction processing versus report processing		
SLN10	1	3	SLN10.1.3	DBMS		The RDBMS shall use history tracking within the database and logging options (e.g., transaction auditing)		
SLN10	1	4	SLN10.1.4	DBMS		The RDBMS shall assure transaction integrity (e.g., rollback, validity checking, referential integrity, other).		
SLN10	1	5	SLN10.1.5	DBMS		The RDBMS 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. The RDBMS must have data replication capabilities to external file formats or other RDBM Systems.		
SLN10	1	12	SLN10.1.12	DBMS		The RDBMS 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). 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.		
SLN10	1	20	SLN10.1.20	DBMS		The RDBMS 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 RDBMS shall provide standard data extraction API to allow import and export of data.		
SLN10	1	23	SLN10.1.23	DBMS		The RDBMS 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 RDBMS shall handle load balancing and/or clustering ability for extended scalability and performance		
SLN10	1	25	SLN10.1.25	DBMS		The RDBMS shall avail the capacity planning model for database configuration.		
SLN10	1	26	SLN10.1.26	DBMS		The RDBMS 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	Notes	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	Specifics	Requirement Description	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		X	Yes (as defined by Oracle)
Siebel Email Marketing Server		X	Yes (as defined by Oracle)
Siebel Campaign Management		X	Yes (as defined by Oracle)
Siebel Web Marketing		X	Yes (as defined by Oracle)
Siebel Marketing Server		X	Yes (as defined by Oracle)
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			One Gate	ECM		MDM	OPA		IdM			Business Intelligence				ESB	Admin			Database		
No.	Role	Liferay	OIM	ESB	FTP	Siebel	BI	IdM	ECM	Liferay Portal	MDM	ESB-WSMAN	ESB-WSINT	AOM	Gateway etc.	Report	OneGate	WCC	Thunderhead	MDM	App	OPM	OIM App	OAM App	DIR App	OBI Pres	Server/Scheduler	ETL	FTP	ESB, OSR, OER	Siebel App Mgmt	Siebel Admin Console	DAC Client	OLTP	OLAP	IdM
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																																					
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

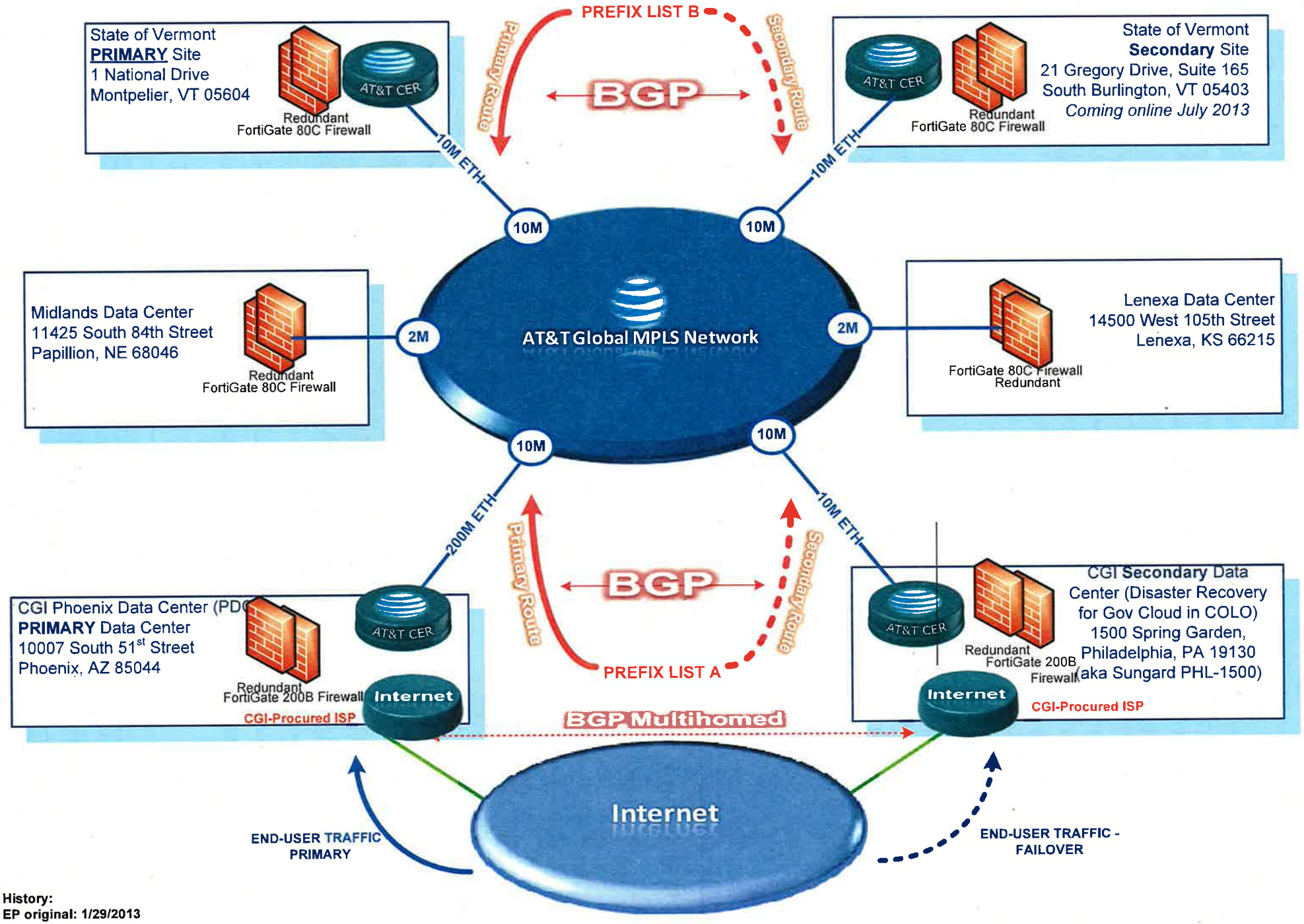
SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)
SLN15 ACCESS Remediation SOW

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Notes	Evidence
SLN15	1	1	SLN15.1.1	Interoperability / Interfaces Requirements	A2.6	The Solution shall have the capability to notify the System administrators/system support staff if an interface is not available for any particular reason. The notification and issue(s) shall be invisible to the applicant/beneficiary/client.		
SLN15	1	2	SLN15.1.2	Interoperability / Interfaces Requirements	A2.8	The Solution shall implement, at a minimum, interfaces (both real-time or batch) with the applications and data sources listed in "Interface List - ACCESS" document included in the procurement library.		
SLN15	1	3	SLN15.1.3	Enterprise Service Bus (ESB) Requirements	P1.15	The Solution must provide for any combination of Alert Destinations such as Email, JMS, SNMP, reporting services, and server logs. The alerts shall be customizable with respect to the frequency of the alert, the ability to enable/disable an alert, rule expiration dates, starting and ending times for an alert, and customizable conditions for an alert".		
SLN15	1	4	SLN15.1.4	Enterprise Service Bus (ESB) Requirements	P1.21	The Solution shall support Transport Security, Message Security, WS-Security, SAML architecture, and WS-Policy. In addition, the Solution shall also implement the ability to externalize security by using a third-party security infrastructure whereby the ESB's proxy action calls a third-party for user/role information.		
SLN15	1	5	SLN15.1.5	Enterprise Service Bus (ESB) Requirements	P1.29	The State of Vermont has invested in the Oracle "stack" and has a strong preference to use this investment to provide the basis of the technology architecture. The State of Vermont is planning to standardize on these products going forward. The State of Vermont and AHS have a strong preference to use Oracle Fusion Middleware (OFM) to provide the SOA infrastructure required for the. The State will consider Solutions using alternative products only where there is a compelling argument to do so provided by the vendor.		
SLN15	1	6	SLN15.1.6	Enterprise Service Bus (ESB) Requirements	P1.30	The Solution must incorporate the ability to undo changes, detect and resolve conflicts, test service connectivity with tracing information, easily enable/disable services, provide logging and view all session activities/change history attributable to each logged in user.		
SLN15	1	7	SLN15.1.7	Data Integration - ETL Requirements	P2.11	The State of Vermont has invested in the Oracle "stack" and has a strong preference to use this investment to provide the basis of the technology architecture. The State of Vermont is planning to standardize on these products going forward. The State of Vermont and AHS have a strong preference to use Oracle Data Integration (ODI) and Oracle Warehouse Builder (OWB). The State will consider Solutions using alternative products only where there is a compelling argument to do so provided by the vendor.		
SLN15	1	8	SLN15.1.8	Master Data Management Requirements	P3.3	The Solution shall enable the delivery of a single client and a single provider view for all stakeholders.		
SLN15	1	9	SLN15.1.9	Master Data Management Requirements	P3.15	Where data is matched by a proxy rather than the actual identifier (e.g. client or provider ID) the Solution shall load data no less quickly, efficiently or accurately.		
SLN15	1	10	SLN15.1.10	Master Data Management Requirements	P3.17	The Solution shall provide tools to validate and manage all client and provider addresses to include all address types (mailing, residential, E-911).		
SLN15	1	11	SLN15.1.11	Master Data Management Requirements	P3.26	The Solution shall integrate with the State Active Directory to provide authorization, e.g., role-based security.		
SLN15	1	12	SLN15.1.12	Master Data Management Requirements	P3.35	The State of Vermont has invested in the Oracle "stack" and has a strong preference to use this investment to provide the basis of the Solution technology architecture. The State of Vermont is planning to standardize on these products going forward. The State of Vermont and AHS expect to implement MDM using a combination of both centralized and registry style implementations and will require strong interactive probabilistic matching capabilities. The State of Vermont has invested in enterprise licenses for Siebel UCM and has created a shortlist of preferred MDM products including Siebel UCM and IBM InfoSphere Standard. The State will consider Solutions using alternative products only where there is a compelling argument to do so provided by the vendor.		
SLN15	1	13	SLN15.1.13	Security Requirements	P4.1	The Solution shall comply with U.S. Department of Health & Human Services and U.S. Department of Education privacy and data security requirements, including, but not limited to, the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act provisions of the American Recovery and Reinvestment Act (ARRA) of 2009.		
SLN15	1	14	SLN15.1.14	Security Requirements	P4.3	The Solution shall implement security controls in accordance with all Federal and State security policy and regulations.		

SLN15	1	15	SLN15.1.15	Security Requirements	P4.4	The Solution shall meet: - Guidance from CMS including MITA Framework 2.0 and Harmonized Security and Privacy Framework		
SLN15	1	16	SLN15.1.16	Security Requirements	P4.5	The vendor shall adhere to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks		
SLN15	1	17	SLN15.1.17	Security Requirements	P4.6	The Solution shall allow for controlled access to participant records. Users will be able to view participant data within the Solution at the State-defined levels of access based on user security privileges.		
SLN15	1	18	SLN15.1.18	Security Requirements	P4.7	The Solution shall provide for security concepts covering the following components: Virtual Private Network (VPN), firewall technology and Demilitarized Zone (DMZ), virus-/intrusion detection, mail/content filtering avoiding fault positives, encryption, Public Key Infrastructure (PKI).		
SLN15	1	19	SLN15.1.19	Security Requirements	P4.8	The Solution shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information.		
SLN15	1	20	SLN15.1.20	Security Requirements	P4.9	Information security shall be built into the Solution from its inception rather than "bolted on" after the Solution Solution has been implemented.		
SLN15	1	21	SLN15.1.21	Security Requirements	P4.10	The Solution shall support security at the object level (e.g. Table, View, Index).		
SLN15	1	22	SLN15.1.22	Security Requirements	P4.11	The Solution shall support security at the row and column level.		
SLN15	1	23	SLN15.1.23	Security Requirements	P4.12	The Solution shall support auditing at the object level (i.e. Table, Column).		
SLN15	1	24	SLN15.1.24	Security Requirements	P4.13	The Solution shall provide the ability for concurrent users to simultaneously view the same record, documentation and/or template.		
SLN15	1	25	SLN15.1.25	Security Requirements	P4.14	The Solution shall provide protection to maintain the integrity of data during concurrent access.		
SLN15	1	26	SLN15.1.26	Security Requirements	P4.15	The software used to install and update the system, independent of the mode or method of conveyance, shall be certified free of malevolent software ("malware"). Vendor may self-certify compliance with this standard through procedures that make use of commercial malware scanning software.		
SLN15	1	27	SLN15.1.27	Security Requirements	P4.16	The Solution shall be configurable to prevent corruption or loss of data already accepted into the Solution in the event of a Solution failure (e.g. integrating with a UPS, etc.).		
SLN15	1	28	SLN15.1.28	Security Requirements	P4.17	The Solution shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Internet Protocol Security (IPsec), XML encryptions, or Secure/Multipurpose Internet Mail Extensions(S/MIME) or their successors.		
SLN15	1	29	SLN15.1.29	Security Requirements	P4.18	The system, when storing PHI on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), shall support use of a standards based encrypted format using 3DES, AES or their successors.		
SLN15	1	30	SLN15.1.30	Security Requirements	P4.20	The Solution shall support a form of user authentication.		
SLN15	1	31	SLN15.1.31	Security Requirements	P4.23	The Solution shall provide the capability to prevent database administrators from seeing the data in databases they maintain.		
SLN15	1	32	SLN15.1.32	Security Requirements	P4.24	The Solution shall support grouping users by functional departments or other organization to simplify security maintenance.		
SLN15	1	33	SLN15.1.33	Security Requirements	P4.25	The Solution shall provide the ability to capture and maintain identifiers required for licensed clinicians to support their practice.		
SLN15	1	34	SLN15.1.34	Security Requirements	P4.26	The Solution shall provide the ability to maintain a directory of all personnel who currently use or access the system/IVR/SQL database.		
SLN15	1	35	SLN15.1.35	Security Requirements	P4.27	The Solution shall provide the ability to create and maintain a directory of external providers to facilitate communication and information exchange.		
SLN15	1	36	SLN15.1.36	Security Requirements	P4.28	The Solution shall provide the ability to identify certain information as confidential (e.g. PII, PHI, etc.) and only make that accessible by appropriately authorized users.		
SLN15	1	37	SLN15.1.37	Security Requirements	P4.29	The Solution shall restrict access to summarized information according to organizational policy, scope of practice, and jurisdictional law.		
SLN15	1	38	SLN15.1.38	Security Requirements	P4.30	The Solution must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user) 2) Role-Based Access Controls (RBAC; users are grouped by role and access rights assigned to these groups) 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)		

SLN15	1	39	SLN15.1.39	Security Requirements	P4.31	The Solution shall provide the ability to prevent specified user(s) or groups from accessing confidential information such as a patient's chart.		
SLN15	1	40	SLN15.1.40	Security Requirements	P4.32	The Solution shall provide the ability to limit access to certain confidential information such as a patient's chart to providers directly involved in service of the patient, or providers involved in review of the service.		
SLN15	1	41	SLN15.1.41	Security Requirements	P4.33	When access to a user's account is restricted, the Solution shall provide a means for appropriately authorized users to "break the glass" and obtain access for emergency situations, as defined by Vermont policy.		
SLN15	1	42	SLN15.1.42	Security Requirements	P4.34	When access to a chart is restricted and the "break the glass" has occurred, the Solution shall provide the ability to notify specified users and provide an audit trail for this access.		
SLN15	1	43	SLN15.1.43	Security Requirements	P4.35	The Solution shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups or processes acting on behalf of users, for the performance of specified tasks.		
SLN15	1	44	SLN15.1.44	Security Requirements	P4.36	The Solution shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.		
SLN15	1	45	SLN15.1.45	Security Requirements	P4.37	The Solution shall support removal of a user's privileges without deleting the user from the Solution to ensure history of user's identity and actions.		
SLN15	1	46	SLN15.1.46	Security Requirements	P4.38	The Solution shall be able to support RBAC in compliance with the HL7 Permissions Catalog.		
SLN15	1	47	SLN15.1.47	Security Requirements	P4.39	The Solution shall be capable of operating within an RBAC infrastructure conforming to ANSI INCITS 359-2004, American National Standard for Information Technology – Role Based Access Control.		
SLN15	1	48	SLN15.1.48	Security Requirements	P4.40	The Solution shall provide more-advanced session management abilities such as prevention of duplicate logins, remote logout and location-specific session timeouts.		
SLN15	1	49	SLN15.1.49	Security Requirements	P4.41	The Solution shall provide the ability to perform Solution administration functions such as reference table maintenance and adding / removing users from the system.		
SLN15	1	50	SLN15.1.50	Security Requirements	P4.42	The Solution shall allow users access based on their roles irrespective of their geographical location.		
SLN15	1	51	SLN15.1.51	Security Requirements	P4.43	The Solution shall provide the capability to integrate with existing authentication and authorization mechanisms (RACF on the mainframe).		
SLN15	1	52	SLN15.1.52	Security Requirements	P4.44	The Solution shall provide the capability to create temporary and emergency accounts and terminate those accounts automatically after a user defined period of time.		
SLN15	1	53	SLN15.1.53	Security Requirements	P4.45	The Solution shall provide the capability to override a role and restrict access to information by users or groups of users.		
SLN15	1	54	SLN15.1.54	Security Requirements	P4.46	The Solution shall allow an individual with active eligibility under a different user id to reapply under their own user id.		
SLN15	1	55	SLN15.1.55	Security Requirements	P4.47	The Solution shall provide the capability to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.		
SLN15	1	56	SLN15.1.56	Security Requirements	P4.48	The Solution shall provide the capability to identify and report on inappropriate access to information in the system, based on user defined criteria.		
SLN15	1	57	SLN15.1.57	Security Requirements	P4.49	The State of Vermont has invested in the Oracle "stack" and has a strong preference to use this investment to provide the basis of the Solution technology architecture. The State of Vermont is planning to standardize on these products going forward. The State of Vermont and AHS have a strong preference to use Oracle Identity Manager (OIM) to provide the security management required for the Solution. The State will consider Solutions using alternative products only where there is a compelling argument to do so provided by the vendor.		
SLN15	1	58	SLN15.1.58	Identity Management Requirements	P15.1	The Solution shall support single sign-on capability for all users.		
SLN15	1	59	SLN15.1.59	Identity Management Requirements	P15.2	The Solution shall provide APIs/Connectors to integrate with a variety of 3rd party/custom applications to provide single sign-on.		
SLN15	1	60	SLN15.1.60	Identity Management Requirements	P15.3	The Solution shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The Solution shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).		
SLN15	1	61	SLN15.1.61	Identity Management Requirements	P15.4	When passwords are used, the Solution shall provide an administrative function that resets passwords.		

SLN15	1	62	SLN15.1.62	Identity Management Requirements	P15.5	When passwords are used, the Solution shall not display passwords while being entered.		
SLN15	1	63	SLN15.1.63	Identity Management Requirements	P15.6	The Solution shall provide only limited feedback information to the user during the authentication.		
SLN15	1	64	SLN15.1.64	Identity Management Requirements	P15.7	The Solution shall support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).		
SLN15	1	65	SLN15.1.65	Identity Management Requirements	P15.8	When passwords are used, the Solution shall allow an authenticated user to change their password, automatically when possible, consistent with password strength rules.		
SLN15	1	66	SLN15.1.66	Identity Management Requirements	P15.10	When passwords are used, the Solution shall support case-sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).		
SLN15	1	67	SLN15.1.67	Identity Management Requirements	P15.11	When passwords are used, the Solution shall use either standards-based encryption, e.g., 3DES, AES, or standards-based hashing, e.g., SHA1 to store or transport passwords.		
SLN15	1	68	SLN15.1.68	Identity Management Requirements	P15.13	The Solution shall meet: NIST 800-63 guidance, CMS E-Authentication Assurance Levels – From CMS Level 1: Single factor authentication, Identity proofing relies on subscriber's own assertions Level 2: Single factor authentication, requires verifying the individual's financial account information, and other information Level 3: Multifactor authentication, requires verifying the individual's financial account information, and other information Level 4: Multifactor authentication, In-person proofing is required Tokens (typically a cryptographic key or password) for proving identity, Identity proofing, registration and the delivery of credentials which bind an identity to a token, Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be Assertion mechanisms used to communicate the results of a remote authentication to other parties.		
SLN15	1	69	SLN15.1.69	Identity Management Requirements	P15.14	The Solution shall re-authenticate the user before any access to Protected Health Information (PHI) or other sensitive or confidential information is allowed, including when not connected to a network (e.g. on unconnected mobile devices).		
SLN15	1	70	SLN15.1.70	Identity Management Requirements	P15.15	The Solution shall encrypt all storage of all passwords using a one-way hash or other equivalent functionality to minimize damage from a security breach.		



History:
EP original: 1/29/2013
Chase Heath: 3/21/13
EP: 3/22/2013

Internet Prevention System (IPS)

HEALTHCARE ENTERPRISE SERVICES PLATFORM

Health Benefits Exchange View

Non Production Environments (Development, Testing and Training)

Version 3 05242013

Architectural Requirements

1. Segregate application services and installs (minimize running everything on one server in production, staging or Disaster Recovery)
2. Clearly define security boundaries between users, web (dmz, WAN), application and database zones.
3. Design for quick and predictable vertical and horizontal scaling.
4. Vertical scaling through more cpu, mem, disk, virtual infrastructure
5. Horizontal scaling through load balanced web, application and database instances
6. Segregate database workloads based on usage. OLTP(Transactional), versus OLAP(Star Schema) versus Other(Security).
7. Testing is the only environment that is approved to have external internet traffic for SFTP or ESB service testing. No other external connectivity is allowed.
8. All interactions between autonomous applications will utilize Enterprise Service Bus for data access.
9. 100% virtualization using VMWare 5.X or higher.
10. All DMZ network traffic to traverse CGI Internet.
11. All traffic to traverse secure MPLS WAN network established and maintained by CGI between SOV and CGI data centers and vendors.
12. Development, Testing and Training are mirrors of each other.
13. Oracle database instances are separate virtual machines each with a single instance of oracle installed.
14. No high availability is required in non production other than VMWare vMotion will be in place and tested to mitigate hardware failures.

GREEN = USERS

YELLOW = VIRT SRVS

PURPLE = WAN SECURITY ZONES

RED = DMZ SECURITY ZONES

BLUE = PHYS SRVS

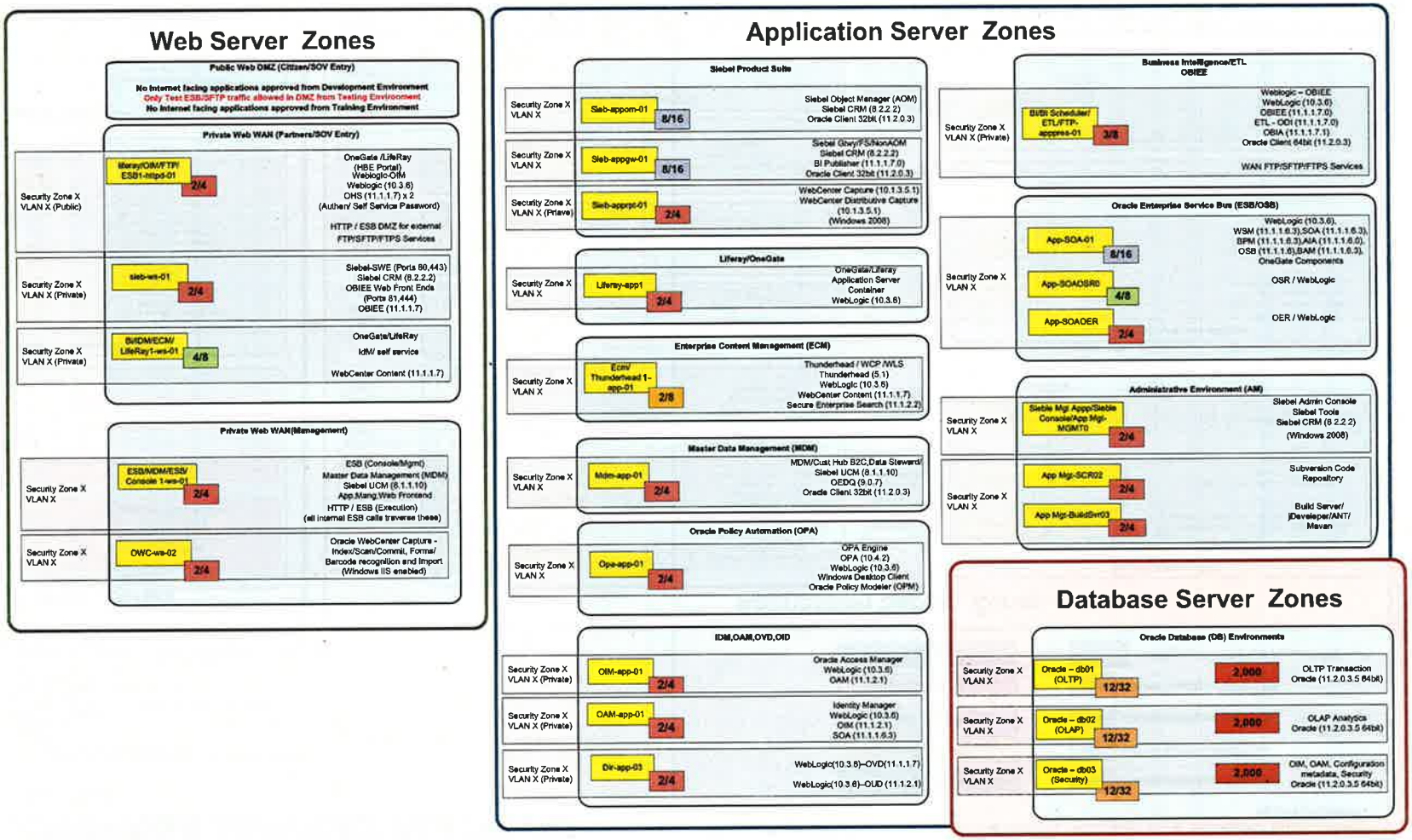
2/4 CGI VM 2vCPU w/4GB RAM

4/8 CGI VM 4vCPU w/8GB RAM

8/16 CGI VM 8vCPU w/16GB RAM

12/32 CGI VM 12vCPU w/32GB RAM

SAN GB CGI Storage in GB (DB & Apps/ COTS)



HEALTHCARE ENTERPRISE SERVICES PLATFORM

Health Benefits Exchange View

Production Environments (Production, Staging and Disaster Recovery)

Version 3 05242013

Architectural Requirements

1. Segregate application services and installs (minimize running everything on one server in production, staging or Disaster Recovery)
2. Clearly define security boundaries between users, web (dmz, WAN), application and database zones
3. Design for quick and predictable vertical and horizontal scaling
4. Vertical scaling through more cpu, mem, disk, virtual infrastructure
5. Horizontal scaling through load balanced web, application and database instances
6. Segregate database workloads based on usage. OLTP(Transactional), versus OLAP(Star Schema) versus Other(Security).
7. Physical Servers utilized in 3 separate Clusters of 2 Oracle RAC nodes each.
8. All interactions between autonomous applications will utilize Enterprise Service Bus for data access.
9. 100% virtualization using VMWare 5.X or higher other than 6 physical database servers.
10. All DMZ network traffic to traverse CGI Internet.
11. All other traffic to traverse secure MPLS WAN network established and maintained by CGI between SOV and CGI data centers and vendors.
12. Staging and Disaster Recovery environments mirror the production environment.

GREEN = USERS

YELLOW = VIRT SRVS

PURPLE = WAN SECURITY ZONES

RED = DMZ SECURITY ZONES

BLUE = PHYS SRVS

CGI VM 2vCPU w/4GB RAM

4/8 CGI VM 4vCPU w/8GB RAM

8/16 CGI VM 8vCPU w/16GB RAM

12/32 CGI VM 12vCPU w/32GB RAM

SAN GB CGI Storage in GB (DB & Apps/ COTS)

Web Server Zones

Public Web DMZ (Citizen/SOV Entry)

Security Zone X VLAN X (Public)
- liferay/oim-httpd-01, liferay/oim-httpd-02 (2/4) — OneGate /LifeRay (HBE Portal) Weblogic-OIM Weblogic (10.3.6) (Authen/ Self Service Password)

Security Zone X VLAN X (Public))
- esb-wsdmz-01, esb-wsdmz-02 (2/4) — HTTP / ESB DMZ for external

Security Zone X VLAN X (Public))
- sFtp-01 (2/4) — FTP/SFTP/FTPS Services

Private Web WAN (Partners/SOV Entry)

Security Zone X VLAN X (Private)
- siebel-ws-01, siebel-ws-02 (2/4) — Siebel-SWE (Ports 80,443) Siebel CRM (8.2.2.2) OBIEE Web Front Ends (Ports 81,444) OBIEE (11.1.1.7)
- Bi/Idm/Ecm-ws-01, Bi/Idm/Ecm-ws-02 (4/8) — IdM/ self service Enterprise Content Management (ECM) Web Frontend WebCenter Content (11.1.1.7)

Security Zone X VLAN X (Private)
- liferay-portal-01, liferay-portal-02 (2/4) — OneGate/LifeRay

Private Web WAN(Management)

Security Zone X VLAN X (Private)
- Esb/Mdm1-wsman-01 (2/4) — ESB (Console/Mgmt) Master Data Management (MDM) Siebel UCM (8.1.1.10) App.Mang Web Frontend

Security Zone X VLAN X (Private)
- Esb/Mdm1-wsint-01, Esb/Mdm2-wsint-02 (2/4) — HTTP / ESB (Execution) (all internal ESB calls traverse these)

Security Zone X VLAN X
- OWC-ws-02 (2/4) — Oracle WebCenter Capture - Index/Scan/Commit, Forms/ Barcode recognition and Import (Windows IIS enabled)

Temp Server

Security Zone X VLAN X
- VTHIX1stgUTL01 (2/4) — Jump Server for initial SW installs

Application Server Zones

Siebel Product Suite

Security Zone X VLAN X
- Sieb-appcm-01, Sieb-appcm-02 (8/16) — Siebel Object Manager (AOM) Siebel CRM (8.2.2.2) Oracle Client 32bit (11.2.0.3)

Security Zone X VLAN X
- Sieb-appgw-01, Sieb-appgw-02 (8/16) — Siebel Gtwy/FS/NonAOM Clustering software Siebel CRM (8.2.2.2) BI Publisher (11.1.1.7.0) Oracle Client 32bit (11.2.0.3)

Security Zone X VLAN X
- Sieb-appcpt-01 (2/4) — WebCenter Capture (10.1.3.5.1) WebCenter Distributive Capture (10.1.3.5.1) (Windows 2008)

Security Zone X VLAN X
- Sieb-appcti-01 (2/4) — Siebel CTI Server (Windows 2008)

Liferay/OneGate

Security Zone X VLAN X
- Liferay-app1, Liferay-app2 (4/16) — OneGate/Liferay Application Server Container OneGate/Liferay (3.2.1) Weblogic (10.3.5)

Enterprise Content Management (ECM)

Security Zone X VLAN X
- Ecm/Thunderhead-1, Ecm/Thunderhead-2 (4/16) — Thunderhead (5.1) / WCP /WLS WebLogic (10.3.6) WebCenter Content (11.1.1.7) Secure Enterprise Search (11.1.2.2)

Master Data Management (MDM)

Security Zone X VLAN X
- Mdm-app-01, Mdm-app-02 (2/4) — MDM/Cust Hub B2C,Data Steward/ Siebel UCM (8.1.1.10) OEDQ (9.0.7) Oracle Client 32bit (11.2.0.3)

Oracle Policy Automation (OPA)

Security Zone X VLAN X
- Opa-app-01, Opa-app-02 (4/16) — OPA Engine OPA (10.4.2)

Security Zone X VLAN X
- Client OPM (Not VM only Client Machine Install) — Windows Desktop Client Oracle Policy Modeler (OPM)

IDM,OAM,OVD,OID

Security Zone X VLAN X (Private)
- OIM-app-01, OIM-app-02 (2/4) — Oracle Access Manager (OAM 11.1.2.1)

Security Zone X VLAN X (Private)
- OAM-app-01, OAM-app-02, OAM-app-03 (2/4) — Identity Manager (OIM 11.1.2.1) SOA (11.1.1.6.3)

Security Zone X VLAN X (Private)
- Dir-app-01, Dir-app-02 (2/4) — WebLogic(10.3.6)-OVD(11.1.1.7) WebLogic(10.3.6)-OUD (11.1.2.1)

Business Intelligence/ETL OBIEE

Security Zone X VLAN X (Private)
- BI-appprss-01, BI-appprss-02 (4/8) — OBI Presentation Services Plugin / IBI Presentation Services / OBI Cluster Controller / WebLogic

Security Zone X VLAN X (Private)
- BI-server-01, BI-server-02 (4/8) — OBI Server / OBI Scheduler / OBI Cluster Controller

Security Zone X VLAN X (Private)
- BI Scheduler/ETL/FTP-app-01, BI Scheduler/ETL/FTP-app-02 (2/4) — WAN FTP/SFTP/FTPS Services ETL)

Oracle Enterprise Service Bus (ESB/OSB)

Security Zone X VLAN X
- App-SOA-01, App-SOA-02 (8/16) — OSB / BPM / Coherence / BAM / Healthcare Adaptor / HIPAA Accelerator / WebLogic / FTP
- App-SOAOSR0, App-SOAOSR1 (4/8) — OSR / WebLogic
- App-SOAOER (2/4) — OER / WebLogic

Administrative Environment (AM)

Security Zone X VLAN X
- Sieble Mgt App / Sieble Console/ App Mgt (2/4) — App Mgmt for Siebel Siebel Admin Console (Windows 2008)

Database Server Zones

Oracle Database (DB) Environments — 2,950

Security Zone X VLAN X
- RAC Cluster 1 db-RAC1-02 (12/32) — OLTP Transaction Cluster

Security Zone X VLAN X
- RAC Cluster 2 db-RAC2-02 (12/32) — OLAP Analytics Cluster

Security Zone X VLAN X
- (12/32) — IDM, OAM, Configuration metadata, Security Cluster

Note:
1. Scaling through additional RAC nodes where required.
2. Minimum RAC nodes per cluster shown (2).