EXECUTION VERSION

AMENDMENT NO. 1

TO

MASTER SERVICES AGREEMENT

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

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

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

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

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

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

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

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

STATE OF VERMONT

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

Name: _____

Type or Print

Title: _____

CGI TECHNOLOGIES AND SOLUTIONS, INC.

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

Name: _____

Type or Print

Title: _____

Exhibit C - Critical Milestones

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

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

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

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

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

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

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

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

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

For Critical Milestones categorized as Low:

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

For Critical Milestones categorized as Medium:

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

For Critical Milestones categorized as High:

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

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

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

ATTACHMENT 2
Exhibit D

[see attached]

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

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

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

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

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

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

iii. Web Page Response Time

1. **Definitions.**

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

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

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

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

iv. Response Time for Real Time Transactions

1. **Definitions.**

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

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

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

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

v. Help Desk Mean Time to Resolve Severity Level 1

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

5. Reserved.

ix. Disaster Recovery

1. Definitions.

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

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

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

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

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

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

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

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

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

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

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

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.

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

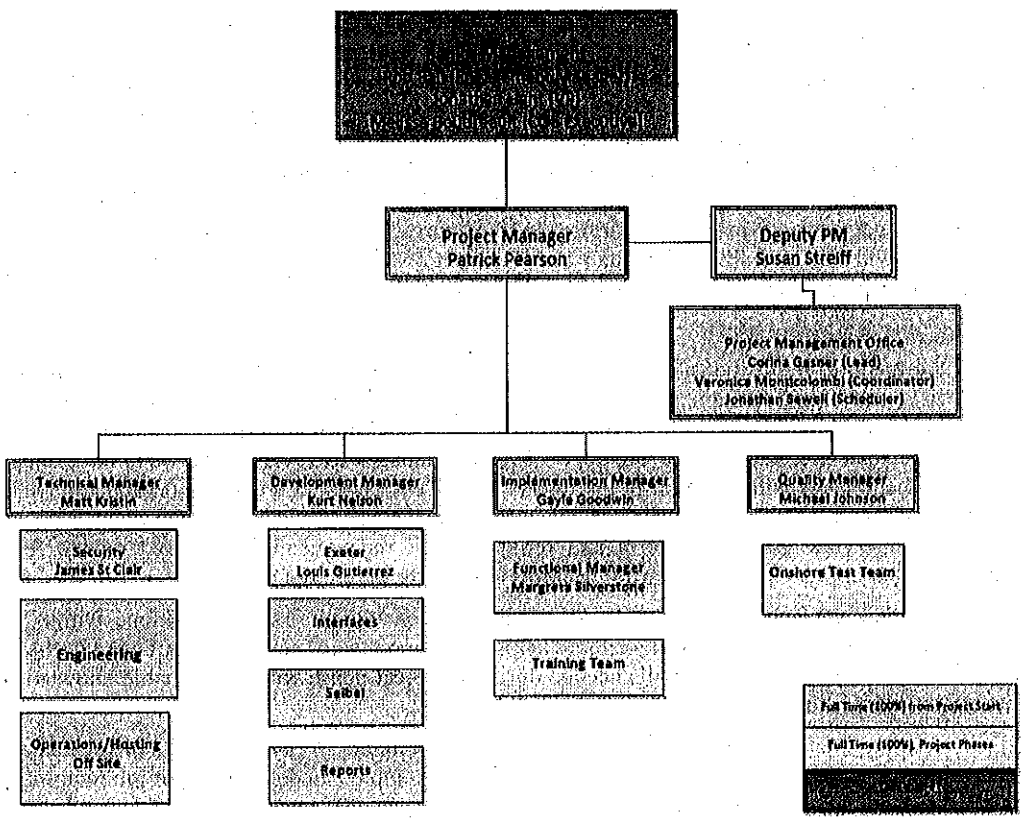
1.1.3. Staffing Assumptions

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:



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

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

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

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

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

1.1.4. Facilities and Access

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

1.1.5. Deliverables & Standards Assumptions

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

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

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.

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.

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

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

Transition and Support Deliverables

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

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

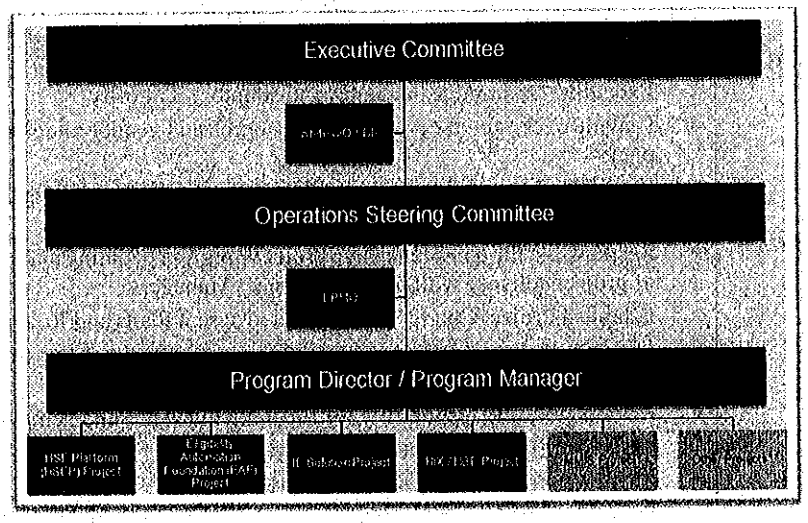
State of Vermont Health Services Enterprise Program Office of IT Projects

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.

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



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

1 Executive Summary

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

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

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

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

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

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

1.2 CGI's Overall Cost Summary

Table 1 summarizes the pricing of our total solution.

Table 1: Mandatory Solution Components

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

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

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

1.4 Table 5.2.3 Ongoing Operations Costs – Base Years

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

Worksheet Notes:

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

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

1.6 Table 5.2.5 Hourly Rate Schedule for Change Orders

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

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

Worksheet Notes:

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

1.7 Table 5.2.6 Summary Schedule of Project Costs

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

Worksheet Notes:

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

1.8 Tables 5.2.7 through 5.2.8.9

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

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

Table 5.2.1. COST PROPOSAL IDENTIFICATION AND INSTRUCTIONS

Contents of the cost proposal must be as follows:

1. **Tab I - Title Page**

   The title page must include the following:

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

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

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

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

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

Table 5.2.2. Detailed Deliverable Cost Schedules

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

Table 5.2.4. Ongoing Operation Costs – Optional Years

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

Table 5.2.6. Summary Schedule of Project Costs

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

Vermont HIX

RFP Section 4.5.1 Call Center Costs

Table 5.2.8.1 Call Center Technology Costs

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

Vermont HIX

RFP Section 4.5.4 Medicaid Plan Selection through the Exchange Solution

Table 5.2.8.2 Medicaid Plan Selection through the Exchange Solution Costs

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

Vermont HIX

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

Table 5.2.8.4 Call Center Staffing and Operation - Base Years Costs

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

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

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

Table 5.2.8.5 Call Center Staffing and Operation - Optional Years Costs

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

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

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

Vermont HIX

RFP Section 4.5.3 Premium Billing Operations - Base Years Costs

Table 5.2.8.7 Individual Premium Billing Operations - Base Years Costs

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

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

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

Operational Costs	Number of Services	Cost Per Month	

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

Vermont HIX

RFP Section 4.5.3 Premium Billing Operations - Base Years Costs

Table 5.2.8.7 Individual Premium Billing Operations - Base Years Costs

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

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

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

Operational Costs Staffing Classification	Number of Staff	Estimated Annual Hours per Staff	Hourly Rate	

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

Vermont HIX

RFP Section 4.5.3 Premium Billing Operations - Optional Years Costs

Table 5.2.8.8 Individual Premium Billing Operations - Optional Years Costs

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

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

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

Operational Costs	Type of Service	Cost Per Month	

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

Vermont HIX

5.2.9.1 Deliverable Pricing

Total Resource First Year Deliverable Value **$32,136,258**

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

Group 1

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

Vermont HIX

5.2.9.2 Milestone Payment Schedule

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

Vermont HIX
5.2.9.4 License Payment Schedule

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

[1] *Licenses to be paid upon installation*

Configuration Total $ 6,507,109.00

5.2.9.6 Payment Schedule Summary

Payment Schedule Summary

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

Amended and Restated Statement of Work No. 1

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

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

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

2. SERVICES TO BE PERFORMED AND SCHEDULE OF PERFORMANCE.

A. Scope of Services

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

B. Location of Services.

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

C. Deliverables and Work Product.

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

D. Milestone Schedule

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

E. Acceptance Criteria and Process.

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

F. Supplier Personnel.

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

---

6. SOFTWARE.

A. Third Party Software provided by Supplier

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

Liferay
OneGate
Thunderhead

B. Third Party Software provided by SOV.

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

---

7. HARDWARE.

Not applicable at this time

---

8. THIRD PARTY CONTRACTS.

NONE AT THIS TIME.

---

9. SERVICE LEVELS.

See Exhibit D attached to the MSA.

---

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

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

---

11. FORECASTING

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

---

12. FACILITIES TO BE PROVIDED BY SUPPLIER.

Not applicable.

---

13. ASSUMPTIONS.

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

SCHEDULE A

RTM

[see attached]

Individual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

ndividual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

Individual Eligibility Requirements Traceability Matrix

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

ndividual Enrollment Requirements Traceability Matrix

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

ndividual Enrollment Requirements Traceability Matrix

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

ndividual Enrollment Requirements Traceability Matrix

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

Individual Enrollment Requirements Traceability Matrix

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

Individual Enrollment Requirements Traceability Matrix

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

ndividual Enrollment Requirements Traceability Matrix

an Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

lan Management Requirements Traceability Matrix

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

lan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

lan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

an Management Requirements Traceability Matrix

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

lan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

lan Management Requirements Traceability Matrix

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

lan Management Requirements Traceability Matrix

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

Plan Management Requirements Traceability Matrix

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

lan Management Requirements Traceability Matrix

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

an Management Requirements Traceability Matrix

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

n Management Requirements Traceability Matrix

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

an Management Requirements Traceability Matrix

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

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

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

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

all Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

all Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

all Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

nall Business Requirements Traceability Matrix

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

Small Business Requirements Traceability Matrix

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

mall Business Requirements Traceability Matrix

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

nancial Management Requirements Traceability Matrix

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

Financial Management Requirements Traceability Matrix

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

Financial Management Requirements Traceability Matrix

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

ıancial Management Requirements Traceability Matrix

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

nancial Management Requirements Traceability Matrix

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

ancial Management Requirements Traceability Matrix

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

nancial Management Requirements Traceability Matrix

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

inancial Management Requirements Traceability Matrix

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

nancial Management Requirements Traceability Matrix

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

Financial Management Requirements Traceability Matrix

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

Financial Management Requirements Traceability Matrix

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

Administrative Requirements Traceability Matrix

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

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

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

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

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

Summarized Reporting Requirements Traceability Matrix

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

Summarized Reporting Requirements Traceability Matrix

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

Summarized Reporting Requirements Traceability Matrix

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

Summarized Reporting Requirements Traceability Matrix

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

Summarized Noticing Requirements Traceability Matrix

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

Summarized Noticing Requirements Traceability Matrix

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

Summarized Noticing Requirements Traceability Matrix

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

Summarized Noticing Requirements Traceability Matrix

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

Summarized Noticing Requirements Traceability Matrix

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

Summarized Noticing Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Technical Requirements Traceability Matrix

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

Web Portal UX Requirements Traceability Matrix

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

Web Portal UX Requirements Traceability Matrix

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

Web Portal UX Requirements Traceability Matrix

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

Consumer Assistance - General Requirements Traceability Matrix

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

Consumer Assistance - General Requirements Traceability Matrix

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

Consumer Assistance - General Requirements Traceability Matrix

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

Consumer Assistance - General Requirements Traceability Matrix

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

Consumer Assistance - Case Management Requirements Traceability Matrix

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

Consumer Assistance - Case Management Requirements Traceability Matrix

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

Navigator Requirements Traceability Matrix

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

Navigator Requirements Traceability Matrix

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

Mandatory Optional Requirements Traceability Matrix

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

Mandatory Optional Requirements Traceability Matrix

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

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

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Definitions

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

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

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

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

	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.

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

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

Base	Level	Sub	Req ID	Focus	Specifics	The Requirement	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-tenent occupancy within building***	no restriction	Allowed only if occupancies are non-hazardous	Allowed if all tenants are data centers or telecommunications companies	Allowed if all tenants are data centers or telecommunications companies	N/A	CGI is Sole tenant	
TIA	1	10	TIA.1.10	Data Center (Architectural)	Building construction	Type of construction	no restriction	no restriction	Type IIA, IIIA, or VA	Type IA or IB	T3		
TIA	1	11	TIA.1.11	Data Center (Architectural)	Building construction	Fire resistive requirements	no requirement	no requirement	no requirement	no requirement	T4		
TIA	1	12	TIA.1.12	Data Center (Architectural)	Building construction	Exterior bearing walls	Code allowable	Code allowable	1 Hour minimum	4 Hours minimum	T3		
TIA	1	13	TIA.1.13	Data Center (Architectural)	Building construction	Interior bearing walls	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	14	TIA.1.14	Data Center (Architectural)	Building construction	Exterior nonbearing walls	Code allowable	Code allowable	1 Hour minimum	4 Hours minimum	T3		
TIA	1	15	TIA.1.15	Data Center (Architectural)	Building construction	Structural frame	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	16	TIA.1.16	Data Center (Architectural)	Building construction	Interior non-computer room partition walls	Code allowable	Code allowable	1 Hour minimum	1 Hour minimum	T4		
TIA	1	17	TIA.1.17	Data Center (Architectural)	Building construction	Interior computer room partition walls	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	18	TIA.1.18	Data Center (Architectural)	Building construction	Shaft enclosures	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	N/A		
TIA	1	19	TIA.1.19	Data Center (Architectural)	Building construction	Floors and floor-ceilings	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T4		
TIA	1	20	TIA.1.20	Data Center (Architectural)	Building construction	Roofs and roof-ceilings	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum	T3		
TIA	1	21	TIA.1.21	Data Center (Architectural)	Building construction	Meet requirements of NFPA 75	No requirements	yes	yes	yes		We believe "yes" but we are not sure.	
TIA	1	22	TIA.1.22	Data Center (Architectural)	Building Components	Vapor barriers for walls and ceiling of computer room	no requirement	yes for walls, no requirement for ceiling	yes	yes	T1	Not required for AZ climate	
TIA	1	23	TIA.1.23	Data Center (Architectural)	Building Components	Building entrances with security checkpoints	no requirement	no requirement	yes (primary building entrance manned)	yes (primary building entrance manned)	T4		
TIA	1	24	TIA.1.24	Data Center (Architectural)	Building Components	Access floor panel construction (when provided)	no requirement	no requirement	computer grade all steel	computer grade all steel or computer grade stell 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	53	TIA.1.53	Data Center (Architectural)	UPS and Battery Rooms	Proximity to computer room	no requirement	no requirement	immediately adjacent	Immediately adjacent	T4		
TIA	1	54	TIA.1.54	Data Center (Architectural)	UPS and Battery Rooms	Fire separation from computer room and other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)	T4		
TIA	1	55	TIA.1.55	Data Center (Architectural)	Required Exit Corridors	Fire separation from computer room and support areas	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)	T4		
TIA	1	56	TIA.1.56	Data Center (Architectural)	Required Exit Corridors	Width	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements and not less than 1.2 m (4 ft) clear	Minimum Code requirements and not less than 1.5 m (5 ft) clear)	T4		
TIA	1	57	TIA.1.57	Data Center (Architectural)	Shipping and receiving areas	Shipping and receiving area Physically separate from other areas of data center	No shipping and receiving area provided	No	yes	yes	T4		
TIA	1	58	TIA.1.58	Data Center (Architectural)	Shipping and receiving areas	Fire separation from other areas of data center	Minimum code requirements if shipping and receiving area present	Minimum code requirement	1 hour	2 hour	T4		
TIA	1	59	TIA.1.59	Data Center (Architectural)	Shipping and receiving areas	Physical protection of walls exposed to lifting equipment traffic	no requirement	no requirement	yes (minimum 19mm (3/4 in) plywood wainscot)	yes (steel bollards or similar protection)	T4		
TIA	1	60	TIA.1.60	Data Center (Architectural)	Shipping and receiving areas	Number of loading docks	no requirement	1 per 2500 sq m / 25,000 sq ft of Computer room	1 per 2500 sq m / 25,000 sq ft of Computer room (2 minimum)	1 per 2500 sq m / 25,000 sq ft of Computer room (2 minimum)	T4		
TIA	1	61	TIA.1.61	Data Center (Architectural)	Generator and fuel storage areas	Proximity to computer room and support areas	no requirement	no requirement	In within Data Center building, provided with minimum 2 hour fire separation from all other areas	Separate building or exterior weatherproof enclosures with Code required building separation	T4		
TIA	1	62	TIA.1.62	Data Center (Architectural)	Generator and fuel storage areas	Proximity to publicly accessible areas	no requirement	no requirement	9 m / 30 ft or greater separation	19 m / 60 ft or greater separation	T2		
TIA	2	1	TIA.2.1	Data Center (Security)	Security	System CPU UPS capacity	na	Building	Building	Building + Battery (8 hour min)	T3		
TIA	2	2	TIA.2.2	Data Center (Security)	Security	Data Gathering Panels (Field Panels) UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)	T4	Security systems on building UPS	
TIA	2	3	TIA.2.3	Data Center (Security)	Security	Field Device UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)	T4	Security systems on building UPS	
TIA	2	4	TIA.2.4	Data Center (Security)	Security	Security staffing per shift	na	1 per 3,000 sq m / 30,000 sq ft (1 minimum)	1 per 2,000 sq m / 20,000 sq ft (2 minimum)	1 per 2,000 sq m / 20,000 sq ft (3 minimum)	T2		
TIA	2	5	TIA.2.5	Data Center (Security)	Security Access Control Monitoring	Generators	industrial grade lock	intrusion detection	card access	card access	T1	plus camera coverage	
TIA	2	6	TIA.2.6	Data Center (Security)	Security Access Control Monitoring	UPS, Telephone & MEP Rooms	industrial grade lock	intrusion detection	card access	card access	T4		
TIA	2	7	TIA.2.7	Data Center (Security)	Security Access Control Monitoring	Fiber Vaults	industrial grade lock	intrusion detection	intrusion detection	card access	N/A	Owned/secured by Telco	
TIA	2	8	TIA.2.8	Data Center (Security)	Security Access Control Monitoring	Emergency Exit Doors	industrial grade lock	monitor	delay egress per code	delay egress per code	T2		
TIA	2	9	TIA.2.9	Data Center (Security)	Security Access Control Monitoring	Accessible Exterior Windows/opening	off site monitoring	intrusion detection (with offsite monitoring during shifts when no security staff is present)	intrusion detection (with offsite monitoring during shifts when no security staff is present)	intrusion detection	T4	Monitored by 24x7x365 on site security	
TIA	2	10	TIA.2.10	Data Center (Security)	Security Access Control Monitoring	Security Operations Center	no requirement	no requirement	card access	card access	T4		
TIA	2	11	TIA.2.11	Data Center (Security)	Security Access Control Monitoring	Network Operations Center	no requirement	no requirement	card access	card access	T4		
TIA	2	12	TIA.2.12	Data Center (Security)	Security Access Control Monitoring	Security Equipment Rooms	no requirement	intrusion detection	card access	card access	T4		
TIA	2	13	TIA.2.13	Data Center (Security)	Security Access Control Monitoring	Doors into Computer Rooms	industrial grade lock	intrusion detection	card or biometric access for ingress and egress	card or biometric access for ingress and egress	T4		
TIA	2	14	TIA.2.14	Data Center (Security)	Security Access Control Monitoring	Perimeter building doors	no monitoring	intrusion detection (with offsite monitoring during shifts when no security staff is present)	card access if main entrance, intrusion detection all others	card access all entrance	T3		
TIA	2	15	TIA.2.15	Data Center (Security)	Security Access Control Monitoring	Main door onto computer room floor	industrial grade lock	card access	Single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential	Single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential, preferably with biometrics.	T2	no man trap but camera covered and biometric	
TIA	2	16	TIA.2.16	Data Center (Security)	Bullet resistant walls, windows & doors	Security Counter in Lobby	na	na	Level 3 (min)	Level 3 (min)	T2		

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

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

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Infrastructure

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

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Networking

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

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

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

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

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

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

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

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

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

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM): Maintenance and Operations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Security General

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

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

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

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

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

Audit Reduction and Report Generation	Y		
Time Stamps	Y		
Protection of Audit Information	Y		
Non-repudiation	Y		
Audit Record Retention	Y		
Audit Generation	Y		
Monitoring for Information Disclosure	Y		
Session Audit	Y		
Hosting Provider can meet all Security Assessment and Authorization measures in the Security Assessment and Authorization Control Group			
Security Assessment and Authorization Policies and Procedures	Y		
Security Assessments	Y		
Information System Connections	Y		
Security Certification (Withdrawn)	Y		
Plan of Action and Milestones	Y		
Security Authorization	Y		
Continuous Monitoring	Y		
Hosting Provider can meet all Configuration Management measures in the Configuration Management Control Group			
Configuration Management Policy and Procedures	Y		
Baseline Configuration	Y		
Configuration Change Control	Y		
Security Impact Analysis	Y		
Access Restrictions for Change	Y		
Configuration Settings	Y		
Least Functionality	Y		
Information System Component Inventory	Y		
Configuration Management Plan	Y		
Hosting Provider can meet all Contingency Planning measures in the Contingency Planning Control Group			
Contingency Planning Policy and Procedures	Y		
Contingency Plan	Y		
Contingency Training	Y		
Contingency Plan Testing and Exercises	Y		
Contingency Plan Update (Withdrawn)	Y		
Alternate Storage Site	Y		
Alternate Processing Site	Y		
Telecommunications Services	Y		

Media Transport	Y		
Media Sanitization	Y		
Hosting Provider can meet all Physical and Environmental Protection measures in the Physical and Environmental Protection Control Group			
Physical and Environmental Protection Policy and Procedures	Y		
Physical Access Authorizations	Y		
Physical Access Control	Y		
Access Control for Transmission Medium	Y		
Access Control for Output Devices	Y		
Monitoring Physical Access	Y		
Visitor Control	Y		
Access Records	Y		
Power Equipment and Power Cabling	Y		
Emergency Shutoff	Y		
Emergency Power	Y		
Emergency Lighting	Y		
Fire Protection	Y		
Temperature and Humidity Controls	Y		
Water Damage Protection	Y		
Delivery and Removal	Y		
Alternate Work Site	Y		
Location of Information System Components	Y		
Information Leakage	Y		
Hosting Provider can meet all Planning measures in the Planning Control Group			
Security Planning Policy and Procedures	Y		
System Security Plan	Y		

Supply Chain Protection	Y		
Trustworthiness	Y		
Critical Information System Components	Y		
Hosting Provider can meet all System and Communications Protection measures in the System and Communications Protection Control Group			
System and Communications Protection Policy and Procedures	Y		
Application Partitioning	Y		
Security Function Isolation	Y		
Information in Shared Resources	Y		
Denial of Service Protection	Y		
Resource Priority	Y		
Boundary Protection	Y		
Transmission Integrity	Y		
Transmission Confidentiality	Y		
Network Disconnect	Y		
Trusted Path	Y		
Cryptographic Key Establishment and Management	Y		
Use of Cryptography	Y		
Public Access Protections	Y		
Collaborative Computing Devices	Y		
Transmission of Security Attributes	Y		
Public Key Infrastructure Certificates	Y		
Mobile Code	Y		

Security Functionality Verification	Y		
Software and Information Integrity	Y		
Spam Protection	Y		
Information Input Restrictions	Y		
Information Input Validation	Y		
Error Handling	Y		
Information Output Handling and Retention	Y		
Predictable Failure Prevention	Y		
Hosting Provider can meet all Program Management measures in the Program Management Control Group			
Information Security Program Plan	Y		
Senior Information Security Officer	Y		
Information Security Resources	Y		
Plan of Action and Milestones Process	Y		
Information System Inventory	Y		
Information Security Measures of Performance	Y		
Enterprise Architecture	Y		
Critical Infrastructure Plan	Y		
Risk Management Strategy	Y		
Security Authorization Process	Y		
Mission/Business Process Definition	Y		

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IRS 1075

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

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

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

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

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

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

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

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

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

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

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

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

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 supervability.			
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.			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM)

Interfaces

Page	Level	Sub	Req ID/New	Focus	Specifics	Requirement Description	Source	Uni-Directional Bi-Directional	Target	Requirement Fulfilled?	Notes	Evidence
SLN5	1	1	SLN5 1.1	Interface General		The HBE solution shall implement the interfaces to and from all specified systems in the SOV EA Requirements Catalog, SLN5 Interfaces per ICD tab and the submitted HBE Interface Control Document						
SLN5	1	2	SLN5 1.2	Interface General		All internal and external application interfaces shall be brokered by the Vermont Integration Hub (VIH)'s ESB and follow ESB standards						
SLN5	1	3	SLN51.3	Interface General		The HBE solution shall implement necessary interfaces to and from the Federal Data Services Hub (CMS - FDSH)						
SLN5	1	4	SLN51.4	Interface General		The HBE solution shall implement necessary interfaces to and from SERFF						
SLN5	1	5	SLN5 1.5	Interface General		The HBE solution shall implement necessary interfaces to and from an external premium processor						
SLN5	1	6	SLN5 1.6	Interface General		The HBE solution shall implement necessary interfaces to and from the existing PeopleSoft/VISION application in Vermont						
SLN5	1	7	SLN5 1.7	Interface General		The HBE solution shall implement necessary interfaces to and from an external interface to support financial management						
SLN5	1	8	SLN5 1.8	Interface General		The HBE solution shall implement necessary interfaces to and from the new Call/Customer Support Center Vendor						
SLN5	1	9	SLN5 1.9	Interface General		The HBE solution shall implement necessary interfaces to and from the SOV centralized document scanning facility						
SLN5	1	10	SLN51.10	Interface General		The HBE solution shall implement necessary interfaces to and from the SOV ACCESS system						
SLN5	1	11	SLN51.11	Physical Interface		Federal Data Services Hub Interface (CMS)	CMS	Bi-Directional	HBE			
SLN5	1	12	SLN51.12	Interface Data Flow		Report: APTC/CSR Payment	CMS	Uni-Directional	HBE			
SLN5	1	13	SLN51.13	Interface Data Flow		Report: Premium Payment History (Monthly)	HBE	Uni-Directional	CMS			
SLN5	1	14	SLN51.14	Interface Data Flow		Enrollment Data - Plan, Premium, APTC/CSR, State Premium Subsidy, State CSR, Household Contribution Amount, HIPP (Monthly)	HBE	Uni-Directional	CMS			
SLN5	1	15	SLN51.15	Interface Data Flow		Publish Carrier and Plan Information (Needed if SERFF interface is not in place)	HBE	Bi-Directional	CMS			
SLN5	1	16	SLN51.16	Interface Data Flow		Provide Plan Non-Renewal, Decertification, and Change in Availability Notices (Needed if SERFF interface is not in place)	HBE	Bi-Directional	CMS			
SLN5	1	17	SLN51.17	Interface Data Flow		Provide Rate and Benefit Data (Needed if SERFF interface is not in place)	HBE	Bi-Directional	CMS			
SLN5	1	18	SLN51.18	Interface Data Flow		HBE Notifies CMS of Individual Disenrollment from QHP	HBE	Bi-Directional	CMS			
SLN5	1	19	SLN51.19	Interface Data Flow		Validate Individual SSN	HBE	Bi-Directional	CMS			
SLN5	1	20	SLN51.20	Interface Data Flow		CMS or IRS Calculates and Returns Individual MAX APTC Request	HBE	Bi-Directional	CMS			
SLN5	1	21	SLN51.21	Interface Data Flow		Verify Lawful Presence Request, CMS Coordinates with Dept Homeland Security and SSA	HBE	Bi-Directional	CMS			
SLN5	1	22	SLN51.22	Interface Data Flow		Verify Household Income Request, CMS Coordinates with IRS	HBE	Bi-Directional	CMS			
SLN5	1	23	SLN51.23	Interface Data Flow		Initiate Citizenship Verification	HBE	Bi-Directional	CMS			
SLN5	1	24	SLN51.24	Interface Data Flow		Validate Immigration Verification	HBE	Bi-Directional	CMS			
SLN5	1	25	SLN51.25	Interface Data Flow		Send Documentation for Review to Verify Lawful Presence	HBE	Uni-Directional	CMS			
SLN5	1	26	SLN51.26	Interface Data Flow		Verify Individual Unemployment Insurance Request	HBE	Bi-Directional	CMS			
SLN5	1	27	SLN51.27	Interface Data Flow		HBE Reports Individual Exemption Status to IRS through CMS	HBE	Bi-Directional	CMS			
SLN5	1	28	SLN51.28	Interface Data Flow		Verify Employer EIN Request	HBE	Bi-Directional	CMS			
SLN5	1	29	SLN51.29	Interface Data Flow		HBE Notifies of Employer Participation in SHOP Exchange, CMS notifies IRS	HBE	Bi-Directional	CMS			
SLN5	1	30	SLN51.30	Interface Data Flow		HBE Notifies of Employer Termination from Participation in SHOP Exchange, CMS notifies IRS	HBE	Bi-Directional	CMS			
SLN5	1	31	SLN51.31	Interface Data Flow		HBE Notifies CMS of Exchange Appeal Decision, CMS notifies IRS	HBE	Bi-Directional	CMS			
SLN5	1	32	SLN51.32	Interface Data Flow		Provide Plan Quality Rating Methodology	HBE	Bi-Directional	CMS			
SLN5	1	33	SLN51.33	Interface Data Flow		Exchange Financial Statements	HBE	Uni-Directional	CMS			
SLN5	1	34	SLN51.34	Physical Interface		Premium Processor Vendor Interface	HBE	Bi-Directional	Premium Processor			
SLN5	1	35	SLN51.35	Interface Data Flow		Report: Premium Payment History (Monthly)	Premium Processor	Uni-Directional	HBE			
SLN5	1	36	SLN51.36	Interface Data Flow		Enrollment Data - Plan, Premium, APTC/CSR, State Premium Subsidy, State CSR, Household Contribution Amount, HIPP, Individual Public Premium Amount (To be used for Billing)	HBE	Uni-Directional	Premium Processor			
SLN5	1	37	SLN51.37	Interface Data Flow		Underpayment Notification	Premium Processor	Uni-Directional	HBE			
SLN5	1	38	SLN51.38	Interface Data Flow		Late Payment Notification	Premium Processor	Uni-Directional	HBE			
SLN5	1	39	SLN51.39	Interface Data Flow		Individual Public Premium Assistance Billing, Collection Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	40	SLN51.40	Interface Data Flow		APTC/CSR Payment Summaries (based on CMS Report)	Premium Processor	Uni-Directional	VISION			
SLN5	1	41	SLN51.41	Interface Data Flow		State Premium Subsidy Payment Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	42	SLN51.42	Interface Data Flow		User Fee Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	43	SLN51.43	Interface Data Flow		Issuer Payment Remittance Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	44	SLN51.44	Interface Data Flow		Individual Premium (QHP) Billing, Collection Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	45	SLN51.45	Interface Data Flow		Employer Premium (QHP) Billing, Collection Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	46	SLN51.46	Interface Data Flow		State CSR Payment Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	47	SLN51.47	Interface Data Flow		HIPP Payment Transaction Summaries	Premium Processor	Uni-Directional	VISION			
SLN5	1	48	SLN51.48	Interface Data Flow		Refund Remitted Overpayment	Issuers	Uni-Directional	Premium Processor			
SLN5	1	49	SLN51.49	Interface Data Flow		Aggregate Premium Payments	HBE	Uni-Directional	Premium Processor			
SLN5	1	50	SLN51.50	Interface Data Flow		State CSR Funds	DFR	Uni-Directional	Premium Processor			
SLN5	1	51	SLN51.51	Interface Data Flow		State Premium Subsidy Funds	DFR	Uni-Directional	Premium Processor			
SLN5	1	52	SLN51.52	Interface Data Flow		Agent Commissions	Premium Processor	Uni-Directional	Agent			
SLN5	1	53	SLN51.53	Interface Data Flow		Enrollee Invoice Information (Medicaid Plans)	HBE	Uni-Directional	Premium Processor			
SLN5	1	54	SLN51.54	Physical Interface		SERFF Interface	SERFF	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			

SOV Consolidated Non-Functional Requirements Traceability Matrix (RTM) MITA									
Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN6	1	1	SLN6.1.1	Modularity		[Solutions shall] Uses a modular, flexible approach to systems development, including the use of open interfaces and exposed Application Programming Interfaces (API); the separation of standardized business rule definitions from core programming; and the availability of standardized business rule definitions in both human and machine- readable formats. The States commit to formal system development methodology and open, reusable system architecture.			
SLN6	1	2	SLN6.1.2	MITA		States [shall] align to and advance increasingly in MITA maturity for business, architecture, and data by Conducting MITA Self Assessments, Developing MITA Roadmaps, Developing Concept of Operations (COO), and Business Process Models (BPM)			
SLN6	1	3	SLN6.1.3	Industry Standards		[Solutions shall] Ensures alignment with, and incorporation of, industry standards: the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security, privacy and transaction standards; accessibility standards established under section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities, and compliance with Federal Civil Rights laws; standards adopted by the Secretary under section 1104 of the Affordable Care Act; and standards and protocols adopted by the Secretary under section 1561 of the Affordable Care Act. Activity includes the following: Identification of industry standards and Incorporation of industry standards in requirements, development, and testing phases			
SLN6	1	4	SLN6.1.4	Leverage		State solutions should promote sharing, leverage, and reuse of Medicaid technologies and systems within and among States. Activity includes the following: Multi-state efforts, Availability for reuse, Identification of open source, cloud-based, and commercial products, Customization, and Transition and retirement plans			
SLN6	1	5	SLN6.1.5	Business Results		Systems should support accurate and timely processing of claims (including claims of eligibility), adjudications, and effective communications with providers, beneficiaries, and the public. Activity includes the following: Degree of automation, Customer Service, Performance standards and testing			
SLN6	1	6	SLN6.1.6	Reporting		Solutions should produce transaction data, reports, and performance information that contributes to program evaluation, continuous improvement in business operations, transparency, and accountability. Activity includes the following: Accurate data, Interfaces with designated federal repositories or hubs, Automatic generation of reports, Audit trails			
SLN6	1	7	SLN6.1.7	Interoperability		Systems must ensure seamless coordination and integration with the Exchanges (whether run by the state or federal government), and allow interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services. Interactions with the Exchange, Interactions with other entities			

SLN7	1	28	SLN7.1.28	Rules		The Vendor shall assist the State with creating a process and systems capability that posts formal rules to the web for general review by the public.			
SLN7	1	29	SLN7.1.29	Rules		The Vendor shall create the program rules in the proposed Rules Management System and test them in an established environment.			
SLN7	1	30	SLN7.1.30	Rules		The Vendor shall create a valid set of rules to transition from the current mainframe system to the proposed Rules Management system in preparation for the new SOA system.			
SLN7	1	31	SLN7.1.31	Rules		The Vendor rules management team will work with and Mentor the State staff Rule Author(s) in the best practices of: - Converting rules from federal or legislative documents into properly structured rules that can be consumed by the proposed Rules Management System and writing future rules in such a way that eases the transition - Capturing meta-data about each of the rules sets and how they function			
SLN7	1	32	SLN7.1.32	Rules		The Vendor shall provide guidance on: - How best to store and look up the meta-data - Defining the Lifecycle of rule sets - How to integrate or flow rules - How to provide help or commentary on rules - General use of the proposed Rules Management System			
SLN7	1	33	SLN7.1.33	Rules		The Vendor shall provide selected State staff with holistic education on the proposed Rules Management system that includes (but is not limited to): - Knowledge about how the proposed Rules Management system works - Knowledge about how to structure the Rule Author(s) to meet the Agency goals - Knowledge about how to create, maintain and update rules in the proposed Rules Management system			
SLN7	1	34	SLN7.1.34	Rules		Solutions shall support mechanisms and ease of use for users to edit rules while maintaining compliance with CMS rules.			
SLN7	1	35	SLN7.1.35	Rules		The Vendor must follow all standards defined by CMS in Guidance for Exchange and Medicaid Technology Systems and Enhanced Funding Requirements: Seven Conditions and Standards; and other federal guidelines yet to be defined; including use a technology neutral rules repository.			
SLN7	1	36	SLN7.1.36	Rules		Solutions shall support design for a multi-step decision			
SLN7	1	37	SLN7.1.37	Rules		Solutions shall have the ability to tune individual steps in the overall decision process for maximum performance by the execution engine			
SLN7	1	38	SLN7.1.38	Rules		Solutions shall support reporting requirements either natively or integrate with other reporting tools to provide reporting			
SLN7	1	39	SLN7.1.39	Rules		Solutions shall support repository infrastructure for rule storage and versioning			

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

Base	Level	Sub	Req ID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN9	1	1	SLN9.1.1			Solutions shall provide the ability to capture solution-generated documents and store them at appropriate level (e.g. individual, case, program, application, various workflow/process)			
SLN9	1	2	SLN9.1.2			Solutions shall ensure version control of documents as they are changed or modified			
SLN9	1	3	SLN9.1.3			Solutions shall allow rollback to a previous version of a document			
SLN9	1	4	SLN9.1.4			Solutions shall enable collaborative document creation and/or markup			
SLN9	1	5	SLN9.1.5			Solutions shall enable attachment of documents to e-mails and e-mail distribution lists			
SLN9	1	6	SLN9.1.6			Solutions shall utilize the solutions authorization and access control for file level security			
SLN9	1	7	SLN9.1.7			Solutions shall have the ability to, based on rules or context, automate the creation of indexing, meta data and overall taxonomy			
SLN9	1	8	SLN9.1.8			Solutions shall have robust bulk load and conversion features			
SLN9	1	9	SLN9.1.9			Solutions shall provide the capability to communicate natively with the document management API			
SLN9	1	10	SLN9.1.10			Solutions shall provide the capability to access the output of the document management system over the Internet and/or Intranet web sites.			
SLN9	1	11	SLN9.1.11			Solutions shall develop a user guide that can be accessed online and printed on demand.			
SLN9	1	12	SLN9.1.12			Solutions shall provide the ability to store electronic forms (solution generated or 3rd-party generated forms)			
SLN9	1	13	SLN9.1.13			Solutions shall provide the capability for online access to policy and procedure and training materials.			
SLN9	1	14	SLN9.1.14			Solutions shall be integrated with document processing center workflow.			
SLN9	1	15	SLN9.1.15			Solutions shall provide scanning software that is configurable to accommodate user-defined field edits such as the exclusion or inclusion of special characters.			
SLN9	1	16	SLN9.1.16			Solutions shall accommodate multiple imaging locations.			
SLN9	1	17	SLN9.1.17			Solutions shall integrate the Imaging and Document Management System with VT HSE Platform.			
SLN9	1	18	SLN9.1.18			Solutions shall provide the capability to access VT HSE Platform to extract data to pre-populate index fields, and/or values on forms.			
SLN9	1	19	SLN9.1.19			Solutions shall provide the capability to send and receive faxed and e-form documents, process the data and image directly into and out of the system including the ability to automatically send confirmation of transmission to the			
SLN9	1	20	SLN9.1.20			Solutions shall provide the capability for performing conditional routing that will send documents to a specific queue or inbox, either manually or electronically, based on preset conditions as defined by the User.			
SLN9	1	21	SLN9.1.21			Solutions shall provide the capability to store and view a multiple page document as a single document.			
SLN9	1	22	SLN9.1.22			Solutions shall provide the capability to attach notes, annotations, e-mails and other documents to an original scanned document at any time without rescanning.			
SLN9	1	23	SLN9.1.23			Solutions shall provide the capability to scan and store imaged documents and electronic files			
SLN9	1	24	SLN9.1.24			Solutions shall provide the capability to notify the user when a duplicate document has been received so the user can decide whether to use the previously received document, replace the existing document or store the new document			
SLN9	1	25	SLN9.1.25			Solutions shall provide the capability to link imaged documentation together and link it to an individual and/or cases within VT HSE Platform.			
SLN9	1	26	SLN9.1.26			Solutions shall provide the capability to record user and workstation identification for each document processed, accessed or updated.			
SLN9	1	27	SLN9.1.27			Solutions shall provide the capability for documents to be grouped together during scanning based on user defined criteria.			
SLN9	1	28	SLN9.1.28			Solutions shall provide the capability to allow the User to manually remove, rescan and replace a previously scanned image or document(s).			

SLN9	1	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			

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

Base	Level	Sub	ReqID New	Focus	Specifics	Requirement Description	Requirement Fulfilled?	Notes	Evidence
SLN10	1	1	SLN10.1.1	DBMS		The System shall lock database records based on various parameters (e.g., at row level, field level, or at the application level).			
SLN10	1	2	SLN10.1.2	DBMS		The System shall have the ability to optimize performance in transaction processing versus report processing			
SLN10	1	3	SLN10.1.3	DBMS		The System shall use history tracking within the database and logging options (e.g., transaction auditing)			
SLN10	1	4	SLN10.1.4	DBMS		The System shall assure transaction integrity (e.g., rollback, validity checking, referential integrity, other).			
SLN10	1	5	SLN10.1.5	DBMS		The System shall handle record locking (e.g., row, field, other) and record updating/committing.			
SLN10	1	6	SLN10.1.6	DBMS		Solutions shall support indexing technology (multiple types of indexing shall be available to tune performance of SQL statement).			
SLN10	1	7	SLN10.1.7	DBMS		Solutions shall provide the ability to optimize individual queries and support parallelizing a query to run on multiple CPUs at the same time to increase performance.			
SLN10	1	8	SLN10.1.8	DBMS		Solutions shall manage multiple query queue entries in parallel.			
SLN10	1	9	SLN10.1.9	DBMS		Solutions shall offer tools to manage and control disparate mixed workloads in a Database Management Solution (DBMS) environment.			
SLN10	1	10	SLN10.1.10	DBMS		The RDBMS must have the ability to maintain security based upon appropriate roles			
SLN10	1	11	SLN10.1.11	DBMS		The RDBMS must have data replication capabilities to external file formats or other RDBM Systems.			
SLN10	1	12	SLN10.1.12	DBMS		The System shall accommodate separate instances of databases.			
SLN10	1	13	SLN10.1.13	DBMS		Solutions shall have full and incremental backup and recovery capabilities on both a regular schedule and an ad hoc basis, including redundant offsite back-ups.			
SLN10	1	14	SLN10.1.14	DBMS		Provide the capability to allow for the continued use of the system during back-ups.			
SLN10	1	15	SLN10.1.15	DBMS		The RDBMS must support geo-encode address data and store geo-data coordinates (longitude and latitude).			
SLN10	1	16	SLN10.1.16	DBMS		Solutions shall assist the State in developing procedures to ensure that specified data is archived and protected from loss, unauthorized access, or destruction.			
SLN10	1	17	SLN10.1.17	DBMS		Solutions shall maintain all data according to state defined records retention guidelines.			
SLN10	1	18	SLN10.1.18	DBMS		Solutions shall maintain all images and electronic documents according to state defined document retention guidelines.			
SLN10	1	19	SLN10.1.19	DBMS		Solutions shall provide on-line access of up to 60 months of data to be used for processing eligibility. Note: Vermont needs to validate # of months			
SLN10	1	20	SLN10.1.20	DBMS		The System shall support online modifications to database structures with minimal user downtime.			
SLN10	1	21	SLN10.1.21	DBMS		The System shall allow for data and transaction replication including, but not limited to, copying an instance of any database to specified locations (e.g. SAN, Multi-site implementations)			
SLN10	1	22	SLN10.1.22	DBMS		The System shall provide standard data extraction API to allow import and export of data.			
SLN10	1	23	SLN10.1.23	DBMS		The System shall provide documented best practices including but not limited to optimum database configuration, client maintenance and change control.			
SLN10	1	24	SLN10.1.24	DBMS		The System shall handle load balancing and/or clustering ability for extended scalability and performance			
SLN10	1	25	SLN10.1.25	DBMS		The System shall avail the capacity planning model for database configuration.			
SLN10	1	26	SLN10.1.26	DBMS		The System supports advanced configurations for data caching (e.g., support of client/application caching, support of server caching etc)			
SLN10	1	27	SLN10.1.27	DBMS		The business analytics solution shall not impact transactional database performance.			

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 procssing workflow.			

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).			

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)

Production Access View

		Public				State Private Network																														
SOV HBE Roles		Public Web DMZ				Private Web WAN					Private Web/WAN Mgmt			Siebel Product Suite			Op e Ga te	ECM		MDM	OPA		IdM			Business Intelligence				ESB	Admin			Database		
No.	Role	Liferay	OIM	ESB	FTP	Siebel	BI	IdM	ECM	Liferay Portal	MDM	ESB W/MAN	ESB W/INT	AOM	Gateway etc	Report	[illegible]	WCC	Thunderhead	MDM	App	OPM	OIM App	OAM App	OIR 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