



# **IT Security Continuous Monitoring Shared Services Security Concept of Operations (SECONOPS)**

**Version 1.0**

**December 2015**



**Homeland  
Security**

## Revision/Change Record

Revision	Date	Revision/Change Description	Section/Pages Affected
D0.11	November 12, 2014	Initial Draft	All
D0.14	December 5, 2014	Addressed FNR and Stakeholder Comments.	All
D0.15	March 13, 2015	Revised to align with IT Security Continuous Monitoring Shared Services Design Document.	All
D0.16	June 11, 2015	Revised to reflect ITSCM Shared Services	All
D0.17	June 24, 2015	Revised to reflect changes to address DHS OGC concerns	All
D0.18	June 24, 2015	Updated graphics to reflect ITSCM Shared Services	All
D0.19	September 2015	Added statement regarding the document does not have any connection with technical requirements of any acquisition	New page 9
D0.20	October 16, 2015	Addressed revisions as suggested by OGC	All (tracking document available)
D1.0	December 7, 2015	Prepared for uploading to US-CERT.gov	

## Table of Contents

<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 What is a “Shared Service?” .....	1
1.2 Purpose and Scope.....	2
1.3 Background .....	2
1.4 IT Security Continuous Monitoring Shared Services Mission Objective .....	3
1.5 Document Organization .....	3
1.6 Assumptions.....	4
<b>2. OPERATIONAL VIEW .....</b>	<b>6</b>
<b>3. ROLES AND RESPONSIBILITIES .....</b>	<b>8</b>
<b>4. THE IT SECURITY CONTINUOUS MONITORING SHARED SERVICES LIFECYCLE.....</b>	<b>1</b>
4.1 IT Security Continuous Monitoring Shared Services Phase 1: Service Strategy.....	2
4.1.1 Roles .....	3
4.1.2 Responsibilities.....	3
4.1.3 Assumptions.....	3
4.1.4 Outputs.....	4
4.2 IT Security Continuous Monitoring Shared Services Phase 2: IT Security Continuous Monitoring Shared Services Service Design .....	4
4.2.1 Roles .....	5
4.2.2 Responsibilities.....	6
4.2.3 Risks.....	6
4.2.4 Security Strategy.....	6
4.2.5 Assumptions.....	7
4.2.6 Outputs from this Phase .....	7
4.3 IT Security Continuous Monitoring Shared Services Phase 3: Service Testing and Evaluation.....	8
4.3.1 Roles .....	9
4.3.2 Responsibilities.....	9
4.3.3 Risks.....	9
4.3.4 Security Strategy.....	10
4.3.5 Assumptions.....	10
4.3.6 Outputs.....	10
4.4 IT Security Continuous Monitoring Shared Services Phase 4: Service Transition... 11	
4.4.1 Roles .....	12

4.4.2	Responsibilities.....	12
4.4.3	Risks.....	13
4.4.4	Security Strategy.....	13
4.4.5	Assumptions.....	13
4.4.6	Outputs.....	13
4.5	IT Security Continuous Monitoring Shared Services Phase 5: IT Security Continuous Monitoring Shared Services Operations.....	14
4.5.1	Roles & Responsibilities.....	14
4.5.2	Risks.....	15
4.5.3	Security Strategy.....	16
4.5.4	Assumptions.....	18
4.6	IT Security Continuous Monitoring Shared Services Phase 6: Service Improvement.....	18
4.6.1	Roles.....	19
4.6.2	Responsibilities.....	19
4.6.3	Risks.....	19
4.6.4	Security Strategy.....	20
4.6.5	Assumptions.....	22
4.6.6	Outputs.....	22
4.7	IT Security Continuous Monitoring Shared Services Phase 7: End of Life: IT Security Continuous Monitoring Shared Services Transition Out.....	22
4.7.1	Roles.....	23
4.7.2	Responsibilities.....	23
4.7.3	Risks.....	23
4.7.4	Security Strategy.....	23
4.7.5	Assumptions.....	24
4.7.6	Outputs.....	24
<b>5.</b>	<b>PORTAL (LOCATION, PROTECTION, AND AVAILABILITY).....</b>	<b>25</b>
<b>6.</b>	<b>REFERENCES, ACRONYMS, AND ABBREVIATIONS.....</b>	<b>26</b>
6.1	References.....	26
6.2	Acronyms and Abbreviations.....	27
<b>APPENDIX A: MISSION ATTRIBUTES AND MISSION ASSURANCE</b>		
	<b>PRINCIPLES.....</b>	<b>28</b>
A.1	Protected Attributes/Principles.....	31
A.2	Resilient Attributes/Principles.....	35
A.3	Usable Attributes/Principles.....	36

A.4 Integrity Assured Attributes/Principles .....	36
A.5 Governable Attributes/Principles .....	37
A.6 Manageable Attributes/Principles .....	39
A.7 Trustworthy Attributes/Principles .....	40
<b>APPENDIX B: SERVICE LEVEL AGREEMENTS (SLAS) .....</b>	<b>41</b>
B.1 Common SLOs .....	45
<b>APPENDIX C: USE CASE NARRATIVES.....</b>	<b>63</b>
C.1 Data Collection and Sensor Management .....	65
C.1.1 Data Collection Scenario 1.....	66
C.1.2 Data Collection Scenario 2.....	67
C.1.3 Sensor Management Scenario 1 .....	68
C.2 Portal Scenarios.....	70
C.2.1 Portal Scenario 1 .....	70
C.2.2 Browser Considerations Scenario.....	71
C.2.3 Update Portal Data Scenario 1 .....	72
C.2.4 High Level Tracking and Monitoring of IT Security Continuous Monitoring Shared Services Scenario 1 .....	73
C.2.5 O&M and Low Level Tracking and Monitoring of IT Security Continuous Monitoring Shared Services Scenario 1 .....	74
C.2.6 Access to Audit Logs Scenario 1.....	74
C.2.7 Access to Audit Logs Scenario 2 .....	75
C.3 Order and Obtain IT Security Continuous Monitoring Shared Services Scenarios..	75
C.3.1 Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 1 .....	75
C.3.2 Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 2 .....	77
C.4 IT Security Continuous Monitoring Shared Services Backup Scenario 1.....	78
C.5 Repair or Replace IT Security Continuous Monitoring Shared Services Component(s).....	79
C.5.1 Repair or Replace IT Security Continuous Monitoring Shared Services Component(s) at Agency Site Scenario 1.....	79
C.5.2 Repair or Replace IT Security Continuous Monitoring Shared Services Component(s) at Agency Site Scenario 2.....	80
C.6 Patch IT Security Continuous Monitoring Shared Services Scenario 1 .....	81
<b>APPENDIX D: IT SECURITY CONTINUOUS MONITORING SHARED SERVICES OPERATIONAL SECURITY PRINCIPLES .....</b>	<b>84</b>
D.1 Protection of Data.....	84

D.2 Location of Data ..... 85

D.3 Communication Link Compromise ..... 85

D.4 Visibility of Data by Shared Service Provider ..... 85

D.5 Visibility of Data by Agency..... 86

D.6 Key Management ..... 86

D.7 Termination or Transfer of Service ..... 86

D.8 Shared Service Provider Notice of Termination ..... 86

D.9 Shared Service Provider Viability ..... 87

D.10 Shared Service Provider Survivability ..... 87

D.11 Protection of Service/System Management Function ..... 87

D.12 Help Desk..... 87

D.13 Availability..... 88

D.14 Hardening..... 88

D.15 Sensor Security Considerations..... 88

D.16 Common Deployment Modes ..... 88

D.17 Vulnerability Data..... 88

D.18 Incident Response ..... 88

D.19 IT Security Continuous Monitoring Shared Services Monitoring ..... 89

D.20 Accountability ..... 89

D.21 Continuous Monitoring and Configuration Management Plan (CMP)..... 90

D.22 Verification of SLA..... 90

D.23 Other SLA Considerations ..... 90

D.24 SLA Enforcement..... 90

D.25 FISMA ..... 90

D.26 IT Security Continuous Monitoring Shared Services Descriptions ..... 91

## List of Tables

Table 1: SECONOPS Document Organization .....	4
Table 2: Document Assumptions.....	4
Table 3: Major Actors in a Shared Environment.....	1
Table 4: Items and Responsibilities .....	2
Table 5: Standards Used .....	26
Table 6: Government Documents Used.....	27
Table 7: IT Security Continuous Monitoring/IT Security Continuous Monitoring Shared Services Documents Used .....	27
Table 8: Commonly Used SLA Terms .....	41
Table 9: Availability SLOs .....	45
Table 10: Response Time SLOs .....	46
Table 11: Capacity SLOs .....	47
Table 12: Capability Indicator SLOs .....	48
Table 13: Support SLOs.....	48
Table 14: Reversibility/Termination Process SLOs .....	49
Table 15: Service Reliability SLOs .....	49
Table 16: Authentication and Authorization SLOs .....	50
Table 17: Cryptography SLOs.....	51
Table 18: Incident Management and Reporting SLOs .....	52
Table 19: Logging and Monitoring SLOs.....	52
Table 20: Auditing and Security Verification SLOs.....	53
Table 21: Vulnerability Management SLOs.....	53
Table 22: Service Changes SLOs .....	54
Table 23: Data Classification SLOs.....	55
Table 24: Data Mirroring, Backup, and Restore SLOs.....	56
Table 25: Data Lifecycle SLOs.....	57
Table 26: Data Portability SLOs.....	57
Table 27: Codes of Conduct, Standards, and Certification Mechanisms SLOs .....	58
Table 28: Purpose Specifications SLOs.....	58
Table 29: Data Minimization SLOs .....	59
Table 30: Use, Retention, and Disclosure Limitation.....	60
Table 31: Openness, Transparency, and Notice.....	60
Table 32: Accountability SLOs .....	61
Table 33: Geographical Location of Shared Service Customer Data .....	62
Table 34: Role Descriptions.....	92

## List of Figures

Figure 1: IT Security Continuous Monitoring Shared Services Notional Overview .....	7
Figure 2: IT Security Continuous Monitoring Shared Services Lifecycle .....	1
Figure 3: Phase 1 IT Security Continuous Monitoring Shared Services Strategy .....	2
Figure 4: IT Security Continuous Monitoring Shared Services Phase 2 Service Design .....	4
Figure 5: IT Security Continuous Monitoring Shared Services Phase 3 Service Testing and Evaluation .....	8
Figure 6: IT Security Continuous Monitoring Shared Services Phase 4 Service Transition .....	11
Figure 7: IT Security Continuous Monitoring Shared Services Phase 5 Operations .....	14
Figure 8: IT Security Continuous Monitoring Shared Services Phase 6 Service Improvement .....	18
Figure 9: IT Security Continuous Monitoring Shared Services Phase 6 Security Attributes .....	20
Figure 10: IT Security Continuous Monitoring Shared Services Service Improvement Security Attributes .....	21
Figure 11: IT Security Continuous Monitoring Shared Services Phase End-of-Life (EOL): Transition Out .....	22
Figure 12: Process for Developing Shared Service High Baseline .....	29
Figure 13: High Security Baseline Attributes for a Shared Service .....	30
Figure 14: IT Security Continuous Monitoring Shared Services Overview for Narrative Use Cases .....	64
Figure 15: IT Security Continuous Monitoring Shared Services, Agency, and Shared Service Provider Data Locations .....	65
Figure 16: Data Collection Scenario 1 Sequence Diagram .....	67
Figure 17: Data Collection Scenario 2 Sequence Diagram .....	68
Figure 18: Sensor Management Scenario 1 .....	69
Figure 19: Sensor Management Scenario 1 Sequence Diagram .....	70
Figure 20: Portal Scenario 1 Sequence Diagram .....	71
Figure 21: Update Portal Scenario 1 .....	73
Figure 22: Access to Audit Logs Scenario 1 Sequence Diagram .....	74
Figure 23: Access to Audit Logs Scenario 2 Sequence Diagram .....	75
Figure 24: Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 1 Sequence Diagram .....	77
Figure 25: Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 2 Sequence Diagram .....	78
Figure 26: IT Security Continuous Monitoring Shared Services Backup Scenario 1 Sequence Diagram .....	79
Figure 27: Repair or Replace IT Security Continuous Monitoring Shared Services Component(s) at Agency Site Scenarios 1 Sequence Diagram .....	80

Figure 28: Repair or Replace IT Security Continuous Monitoring Shared Services Component(s)  
at Agency Site Scenarios 2 Sequence Diagram .....81

Figure 29: Patch IT Security Continuous Monitoring Shared Services Scenario 1.....83

Please Note: This document is not intended to be interpreted as constituting contractual requirements with respect to any ongoing or upcoming (specifically TO2F) Continuous Diagnostics and Mitigation (CDM) procurements.

## **Executive Summary**

This Security Concept of Operations (SECONOPS) explores the considerations of implementing **Information Technology security** as a Shared Service. Specifically, it examines how an Information Technology (IT) Security Continuous Monitoring program could be implemented and how it would function as a Shared Service. It answers the following questions that may be most important to an Agency:

- What are the potential benefits of an IT Security Continuous Monitoring Shared Service?
- What are the security principles that should govern an ITSCM Shared Service?
- What are the lifecycle phases for deployment and implementation of such a Shared Service?
- Who would be responsible for different elements of the Shared Service?
- What are the Service Level Objectives that could be used to govern a Shared Service to ensure that the Agencies are receiving the level of security and transparency that they require?

The Chief Information Officer (CIO) Council, “Federal Shared Services Implementation Guide,” dated April 16, 2013, lists potential benefits that the Federal Government could realize by implementing shared services. These benefits are as follows:

- Enhance awareness and adoption of available shared services across the government;
- Promote agility and innovation within Agencies by improving speed, flexibility, and responsiveness to provisioning services through a “Shared-First” approach;
- Focus more Agency resources on core mission requirements rather than administrative support services;
- Embrace the adoption of best practices and best-in-class ideas and innovations;

The main body of this SECONOPS provides an introduction to “Shared Services,” roles and responsibilities and the lifecycle that will take IT Security Continuous Monitoring Shared Services from strategy through design, implementation, operations, service improvement and eventually end-of-life. The appendices contain the details of how the security attributes for IT Security Continuous Monitoring Shared Services were developed, and the security principles and Service Level Objectives (SLOs) that could be applicable to IT Security Continuous Monitoring Shared Services. Additionally, Use Case sequence diagrams are provided to view the intended conceptual interactions of the major actors in IT Security Continuous Monitoring Shared Services. The IT Security Continuous Monitoring Shared Services SECONOPS is intended to provide useful security concepts that will be considered in subsequent design, testing and operations.

## 1. Introduction

This SECONOPS was written for the Agencies who would like to learn more about the intended security objectives of the Shared Service that will provide IT Security Continuous Monitoring Shared Services and ultimately other security services. The majority of this SECONOPS will focus on IT Security Continuous Monitoring Shared Services, but it is almost equally applicable to any Shared Service for the Federal Government required to meet a High Security Baseline<sup>1</sup>. The emphasis in this SECONOPS is not on the specifics of the service provided by IT Security Continuous Monitoring, but on the delivery mechanism of the “Shared Service.” To state this in another way, this SECONOPS deals with the intended security infrastructure, principles and suggested SLOs to ensure that the service package is being delivered securely and in accordance with Federal requirements.

### 1.1 What is a “Shared Service?”

According to the Executive Office of the President, “Federal Information Technology Shared Service Strategy,” dated May 2, 2012, *“An IT shared service is defined as: An information technology function that is provided for consumption by multiple organizations within or between Federal Agencies. There are three general categories of IT shared services: commodity, support, and mission; which are delivered through cloud-based or legacy infrastructure.”*

A Shared Service model offers tremendous potential benefits to the Federal Government. As Agencies face the challenges of greater security threats, evolving technology, increasing standards of security compliance, and tighter budgets, a shared service model could provide great efficiencies of scale. The first step is to identify those security functions that can be automated, because those are functions most likely to transition to a shared service delivery model. If it can be automated, it can be commoditized. According to the Federal Information Technology Shared Service Strategy, commodity IT services are defined as: “a category of back-office IT services whose functionality applies to most, if not all, agencies (e.g., infrastructure and asset management, email, hardware and software acquisition, and help desks).” A security function could be a candidate for commoditization if the task is common to every Agency and technology can do much of the aggregating, sorting, analyzing, and reporting with minimal human intervention. Those security functions that can be commoditized while maintaining or increasing security, will allow Agencies to assign busy security personnel resources to focus on Agency-specific, or challenging security issues. IT Security Continuous Monitoring Shared Services seeks to provide a heavily automated security analysis and reporting functionality, making it an ideal candidate to implement in a shared service environment.

A Shared Service environment changes the security model that has prevailed at most Agencies. Instead of all of the Agencies’ computing resources and data being centralized in their own data centers, the Shared Service model distributes computing infrastructure and data across a wider

---

<sup>1</sup> Information regarding security classifications of Information Technology Systems can be found in the Federal Information Processing Standards (FIPS) 199 publication (<http://csrc.nist.gov/publications/PubsFIPS.html>). Both FedRAMP and NIST have a High Confidentiality, High Integrity, and High Availability controls. Depending on the Agency’s requirements, these controls can be adopted in total or Agency-specific requirements can be specified as needed (e.g. if the application does not need to be operational 24x7 then certain High Availability controls may not be applicable).

geographic and logical boundary. While the infrastructure is distributed, the responsibility for the security of the data still rests with the Agencies. For this reason, it is especially important in a Shared Service environment to make sure the Shared Service Provider (SSP) is held to the same high level of security for the protection of data and the infrastructure as the Agency would insist on for its own infrastructure. This security posture should be defined in contracts that contain Service Level Objectives and/or Service Level Agreements (as appropriate), and the mandated security baseline controls as identified by the FIPS 199 categorization of the data and the system hosting the data. This security posture must be independently tested and verified by the United States (U.S.) Government (USG) Department or Agency (Agencies) providing the shared service through an authorized Third Party Assessment Organization (3PAO) to ensure that the Service Provider is compliant with Agency security regulations.

## **1.2 Purpose and Scope**

The purpose of this SECONOPS is to present the intended security attributes and lifecycle of a Shared Services program. This includes outlining key security approaches to protect Agency data during data acquisition, analysis, and reporting. Where applicable, the IT Security Continuous Monitoring Shared Services framework has been used as a reference point to further illustrate the various steps required in the security lifecycle of a shared service.

The scope of this SECONOPS is relevant to any Agency in the Federal Government that intends to use security shared services such as IT Security Continuous Monitoring Shared Services. The scope includes the users, security officers, program managers, auditors, officers, and the providers of the service. The scope also includes the intended lifecycle of IT Security Continuous Monitoring Shared Services in section 4. The lifecycle of IT Security Continuous Monitoring Shared Services outlines high-level responsibilities, ownership of risks, and projected outputs from each phase of the lifecycle.

## **1.3 Background**

This IT Security Continuous Monitoring Shared Services SECONOPS was developed using inputs from Department of Homeland Security (DHS), Federal Network Resilience (FNR), and Agency representatives, and from a “Top Down” and “Bottoms Up” analysis of security threats, objectives, and controls applicable to the shared services environment. The following is a list of programmatic and operational challenges and considerations that need to be addressed prior to the adoption of shared services:

- Data governance and data security controls
- Protection from Distributed Denial of Service (DDoS)
- Supportability from the service provider
- Liability management in the event of a security breach
- Availability and accessibility of data in the case of a disaster
- Contingency and survivability in the case that the Shared Service Provider ceases operations
- Confidentiality and restrictions on who has access to data

- Privacy<sup>2</sup> and the Fair Information Practice Principles (FIPPs)<sup>3</sup>.
- Storage location for data and applications and Continuity of Operation (COOP)
- Management of data and data remnants
- Cost control
- Legal and Government regulatory compliance

These challenges and considerations were reviewed for their security implications and included in the process for developing the security controls and SLAs/SLOs that will apply to a Shared Service High Security Baseline. The resultant SLA/SLOs language is included in Appendix B: SLAs. Should one or more of the challenges listed, be combined with a viable threat, the challenge could present a security risk to the IT Security Continuous Monitoring Shared Services program and/or system. Development of the High Security Baseline was conducted in parallel with the development of the SECONOPS in order to mitigate these challenges and risks.

Through the use of working group meetings and feedback to SECONOPS artifacts, this document was developed with input from non-Chief Financial Officer (CFO)-Act Agencies due to the relevance of IT Security Continuous Monitoring Shared Services to those Agencies. Agency stakeholder comments and questions have also been aggregated and incorporated into this document where applicable.

Please note that this document does not address acquisition of IT Security Continuous Monitoring Shared Services.

## 1.4 IT Security Continuous Monitoring Shared Services Mission Objective

IT Security Continuous Monitoring Shared Services is intended to provide robust IT Security Continuous Monitoring services to multiple Agencies via a shared service environment, thereby leveraging network and labor resources and lowering the total cost of ownership.

IT Security Continuous Monitoring Shared Services supports the core objectives of IT Security Continuous Monitoring and will offer the following additional benefits:

- Provide Agencies with a secure, efficient, and cost-effective means to obtain IT Security Continuous Monitoring services.
- Reduce the cost of infrastructure support by focusing on mission objectives rather than infrastructure upkeep.
- Provide better, more reliable uptime by leveraging the availability concept of cloud shared services.

## 1.5 Document Organization

Table 1 provides a brief overview of the sections of the SECONOPS and how they support the overall SECONOPS.

---

<sup>2</sup> <http://www.justice.gov/opcl/privacy-act-1974>

<sup>3</sup> <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>

**Table 1: SECONOPS Document Organization**

Section	Description
1. Introduction	
2. Operational View	Presents a potential operational view of IT Security Continuous Monitoring Shared Services and identifies the key high level components and actors.
3. Roles and Responsibilities	Identifies and describes the high level roles and responsibilities
4. The IT Security Continuous Monitoring Shared Services Lifecycle	Describes tasks, roles, responsibilities, assumptions, risks, security strategy, and outputs for each phase. Inherent in this process is embracing Risk Management as the overarching theme which drives the security strategy.
5. Portal	Describes at a high level the portals associated with IT Security Continuous Monitoring Shared Services.
6. References	Lists the relevant industry standards and Government-provided documents and standards used to develop this document.
Apx. A. Mission Attributes and Mission Assurance	Defines the mission attributes and assurance principles for IT Security Continuous Monitoring Shared Services. The attributes provide a common framework for a stakeholder to determine and accept the base principles on which the SECONOPS and the IT Security Continuous Monitoring Shared Services Lifecycle will be based.
Apx. B. Service Level Agreements (SLAs)	Describes common SLOs that should be considered for inclusion in the SLA for the Shared Service Provider, if appropriate.
Apx. C. Use Case Narratives	Describes some of the various high-level, security-relevant notional use case scenarios that IT Security Continuous Monitoring Shared Services may use. The section is intended to bring insight into the considerations that must be addressed when designing IT Security Continuous Monitoring Shared Services
Apx. D. IT Security Continuous Monitoring Shared Services Operational Security Principles	Describes the key Operational Security Principles that a shared service should consider to provide IT Security Continuous Monitoring Shared Services

## 1.6 Assumptions

Table 2 documents and outlines the assumptions and intended roles and responsibilities. Section 4, the IT Security Continuous Monitoring Shared Services Lifecycle, expands on the definition of IT Security Continuous Monitoring Shared Services Strategy and elaborates on Roles and Responsibilities.

**Table 2: Document Assumptions**

Assumptions
The Shared Service Broker will have a combination of acquisitions service provider and customer responsibilities. As an acquisitions service provider, the Shared Service Broker is responsible for acquisitions, contract performance, and operations as defined in the contract. As customer, the Shared Service Broker will be responsible for the strategy, design, and escalation of issues during later phases.

<b>Assumptions</b>
An acquisitions service provider negotiates SLA terms and conditions including dis-incentives for non-performance.
The Contracting Officer enforces the SLA terms and conditions with Shared Service Provider.
The Shared Service provider is responsible for implementing security controls and documenting how exactly the control is implemented. At their discretion, the Shared Service provider may hire an independent third-party assessment organization (3PAO) to perform initial and ongoing verification and validation of the security controls deployed within the Shared Service provider's information system. Typically, the Shared Service provider pays for this 3PAO assessment. Proof of security controls in place does not constitute receipt of an Authority to Operate (ATO).
Individual federal agencies are the only entity that can issue an ATO. The Agency's Authorizing Official will need to ultimately make a risk-based decision to grant an ATO within the agency. The Agency can choose to hire a 3PAO to act as the Shared Services Auditor on behalf of the Agency to conduct a thorough review of the security assessment package to determine that it is complete, consistent, and compliant with requirements. After completing a security assessment, the head of an agency can authorize the system for use, or the ATO.
Authorization and Accreditation will be conducted by the Shared Services system owner pursuant to that Agency's ATO processes. Artifacts from this process may be shared with other Agencies using the Shared Service as an input to their own ATO processes.
The Shared Service Provider provides guidance for opening ports on firewall for egress and ingress of IT Security Continuous Monitoring Shared Services data for Agencies.
The Shared Service Consumer approves and requests the users that have access to IT Security Continuous Monitoring Shared Services metrics and/or are able to track and monitor certain aspects of IT Security Continuous Monitoring Shared Services.
The Shared Service Provider obtains and provides audit logs to support an incident or other required reporting requirements consistent with customer Incident Management Guidance.
Under the IT Security Continuous Monitoring Shared Services Program, Shared Service Provider can provide IT Security Continuous Monitoring Shared Services-compliant sensors to Agencies who request them.
The Shared Service Provider notifies the customer of the results of its information assurance vulnerability alert (IAVA) analysis.
The Shared Service Provider notifies the Federal Risk and Authorization Management Program (FedRAMP), United States Computer Emergency Readiness Team (US-CERT), Shared Service Consumer, and affected Agencies of any incidents that occur with IT Security Continuous Monitoring Shared Services.
IT Security Continuous Monitoring Shared Services Incident Response are coordinated among Agencies and Service Providers in accordance with OMB and US-CERT guidelines.
The "Shared Service Provider Portal User" role is a user designated by the customer to have a need to know to view the IT Security Continuous Monitoring Shared Services Provider asset and vulnerability data.
The Shared Service Provider develops a backup and restoration plan including required restoration time frames.
The Shared Service Consumer (customer paying for the Shared Service) manages the development and implementation of a transition plan to migrate IT Security Continuous Monitoring Shared Services to a new Shared Service Provider should the need arise.
The SLA terms and conditions will be available to Agencies for their input before the SLA is signed. Any executed SLAs will be available via a Portal link or other determined link. An acquisitions service provider and/or DHS will inform Agencies of the Shared Service Provider performance and compliance with the SLAs.

## **2. Operational View**

An operational view provides a description of the interactions between the subject architecture and its environment, and between the architecture and external systems. The purpose of the operational view is to provide a high-level description of what the architecture is supposed to do, and how it is supposed to do it.<sup>4</sup> Please note that “IT Security Continuous Monitoring Shared Services Provider” and “Shared Service Provider” are used interchangeably in this document.

The operational view, shown in Figure 1, depicts a potential operational view, presenting IT Security Continuous Monitoring Shared Services hosted by a Shared Service Provider shown at the top-most cloud, where the Agency Repositories are located. IT Security Continuous Monitoring Shared Services connects to each Agency site(s) via a secure communications path and obtains hardware, software, configuration, and vulnerability data from the Agency’s sensors or possibly through a relay/aggregator. The scanning information from the sensors is retrieved and stored in the corresponding data repository for each Agency. The data for each Agency is segregated in a separate repository so that only the Agency has access to its own data. The data is also segregated from any other entity that the Shared Service Provider might be hosting. Agencies access their data (e.g., asset, vulnerability, metric, log) via one or more portals, including the IT Security Continuous Monitoring dashboard. The Collector portal provides the Agency with access to the IT Security Continuous Monitoring information for the specific configuration that supports the Agency’s IT Security Continuous Monitoring environment. The Dashboard portal allows the Agency to view its part of the Dashboard. The Shared Service Provider portal allows the viewing of the service infrastructure that supports IT Security Continuous Monitoring Shared Services and the Dashboard. Appendix C, “Use Case Narratives,” provides additional details through the description of use case scenarios.

---

<sup>4</sup> DoD Architecture Framework Version 2.0

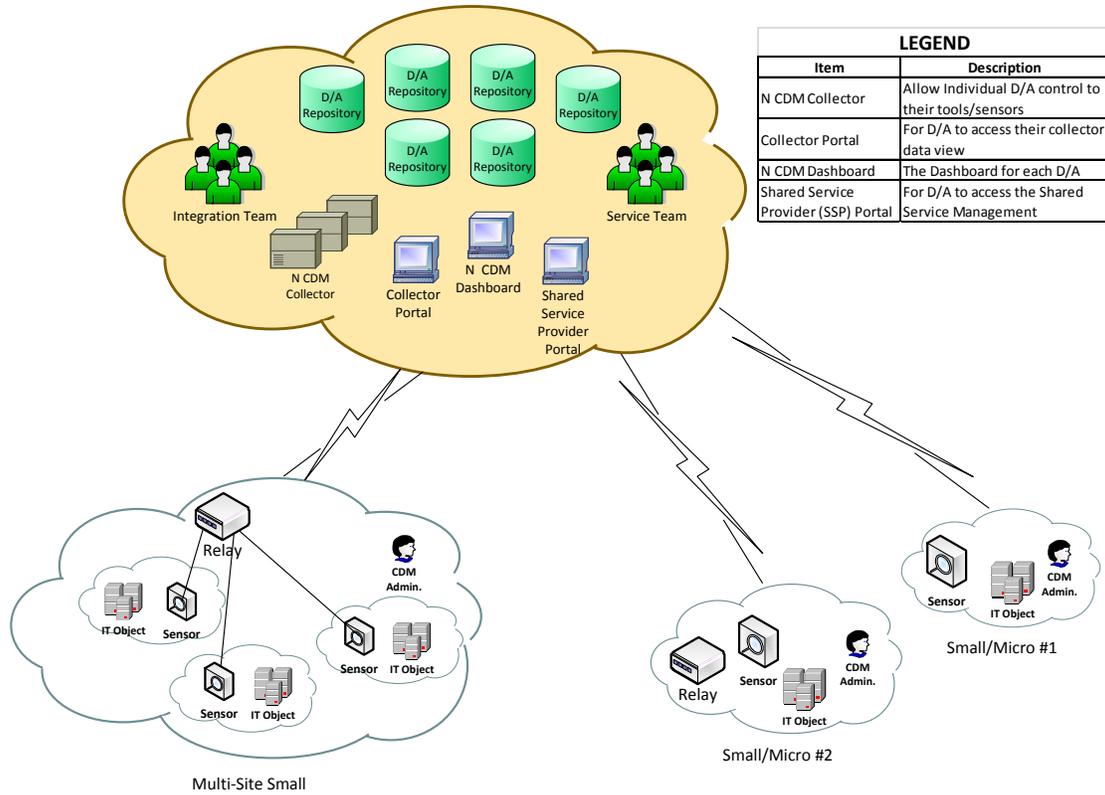


Figure 1: IT Security Continuous Monitoring Shared Services Notional Overview

### **3. Roles and Responsibilities**

The primary security challenge of a shared service environment is that it takes a formerly cohesive system and distributes the components, communications links, data repositories, authorities, responsibilities, and personnel outside of an organization's typical physical boundary as users, servers, and operations personnel may be in different locations. Add to that the complexity of systems supporting more than one customer, and the need for security and segregation of data becomes even more critical to the success of the shared service.

It is important to identify the roles and responsibilities of all actors in a shared service environment so that there are no gaps in security coverage. Though there is no formal consensus across the Federal Government for shared service roles and responsibilities, there are useful references from which IT Security Continuous Monitoring Shared Services actors were defined. Table 3 is derived from extracts from National Institute for Standards and Technology (NIST) Special Publication (SP) 500-292, the Federal IT Shared Services Strategy, and the CIO Council's *Federal Shared Services Implementation*. IT Security Continuous Monitoring Shared Services defined its specific list of shared service actors with very close alignment with NIST because their definitions for cloud services seemed most applicable, clear, and useful to IT Security Continuous Monitoring Shared Services.

Table 3: Major Actors in a Shared Environment

<b>IT Security Continuous Monitoring Shared Services Actor</b>	<b>IT Security Continuous Monitoring Shared Services Definition Adopted from NIST Cloud Definition</b>	<b>IT Security Continuous Monitoring Shared Services Responsibility</b>	<b>Mapping to NIST<sup>5</sup> Cloud Actor</b>	<b>Mapping to Executive Office of the President's Federal IT Shared Services Strategy<sup>6</sup></b>	<b>Mapping to CIO Council's Federal Shared Services Implementation Guide<sup>7</sup></b>
<i>Shared Service Consumer</i>	An organization that uses products provided by the Shared Service Provider. This entity pays for the Shared Service. This entity does not own the Shared Service. A person in this organization is designated as the system owner.	Agencies	Consumer	Customer	Customer/Partner Agency
<i>Shared Service Provider<sup>8</sup></i>	An entity responsible for making a service available to interested parties. This entity receives payment for providing the Shared Service. This entity owns the infrastructure on which the Shared Service is installed.	Government Shared Service Provider or commercial Shared Service Provider	Provider	Supplier	Shared Service Provider

<sup>5</sup> National Institute for Standards and Technology (NIST) Special Publication (SP) 500-292

<sup>6</sup> Chief Information Officer (CIO) Council, *Federal Shared Services Implementation*

<sup>7</sup> Federal Information Technology (IT) Shared Services Strategy

<sup>8</sup> It is possible for an entity to have the role of Shared Service Provider and Shared Service Broker.

IT Security Continuous Monitoring Shared Services Actor	IT Security Continuous Monitoring Shared Services Definition Adopted from NIST Cloud Definition	IT Security Continuous Monitoring Shared Services Responsibility	Mapping to NIST <sup>5</sup> Cloud Actor	Mapping to Executive Office of the President's Federal IT Shared Services Strategy <sup>6</sup>	Mapping to CIO Council's Federal Shared Services Implementation Guide <sup>7</sup>
<i>Shared Service Auditor</i>	A party that conducts independent assessments of shared services, information system operations, performance, and security of the shared service implementation. This entity does not consume the service, does not pay for the service, and does not have any acquisition role.	FedRAMP or Government-designated third party auditor (3PAO).	Auditor	N/A	N/A
<i>Shared Service Broker<sup>9</sup></i>	An entity that manages the performance and delivery of Shared Services, and negotiates the relationships between Shared Service Consumer and Shared Service Providers. This entity does not own the Shared Service.	Acquisitions service provider	Broker	Managing Partner	Managing Partner

Table 4 presents the major items and responsibilities for the IT Security Continuous Monitoring Shared Services primary stakeholders. Authorization and Accreditation will be conducted by the Shared Services consumer pursuant to that Agency's ATO processes. If there are other Agency tenants using the Shared Service, artifacts from this process may be shared with those as an inputs to their own ATO processes.

**Table 4: Items and Responsibilities**

<sup>9</sup> It is possible for an entity to have the role of Shared Service Provider and Shared Service Broker.

Item	Responsibility
Space, power and cooling	Shared Service Provider will provide for all of IT Security Continuous Monitoring Shared Services except those items located at Agency's site (e.g., sensors). Shared Service Provider will provide Agency power and cooling requirements for any components that will be needed at Agency site.
Maintenance of IT Security Continuous Monitoring Shared Services devices at Agencies	If the Shared Service provider installs a component at the Agency location as part of the IT Security Continuous Monitoring Service, the Shared Service provider is responsible for the maintenance of these components. If the Agency provides its own components (e.g., sensors), the Agency is responsible for the maintenance of those components.
Disaster survivability of hosted portion of service	Shared Service Provider
Investment in IT Security Continuous Monitoring Shared Services infrastructure (including people)	Shared Service Provider
Configuration Management (CM) of components supplied by IT Security Continuous Monitoring Shared Services	Shared Service Provider
Operations of hosted portion of service	Shared Service Provider
Ensures Shared Service Provider staff is vetted as appropriate	Shared Service Consumer
Technology update/refresh	Shared Service Provider will provide technology update/refresh of all components provided by IT Security Continuous Monitoring Shared Services.
A&A (the older Certification and Accreditation (C&A) may still be used in some instances)	Authorization and Accreditation will be conducted by the system owner pursuant to that Agency's ATO processes. Agencies may choose to utilize artifacts from this effort and request for additional controls pursuant to their Agency's ATO requirements.
Opening ports on firewall at Agency sites for egress and ingress of IT Security Continuous Monitoring Shared Services data	Agencies with guidance from Shared Service Provider
Mitigation of vulnerabilities	Shared Service Provider is responsible for IT Security Continuous Monitoring Shared Services. Agency is responsible for all components they own and the Agency enterprise.
SLA enforcement	Contracting Officer.

---

<b>Item</b>	<b>Responsibility</b>
Incident <sup>10</sup> response	Shared Service Provider, Agencies, and DHS

---

<sup>10</sup> The specific definition of Incident will be the decision of the organization adopting this CONOPS. Existing definitions can be found in the FISMA 2014 and the Cybersecurity Protection Act of 2014. It is recommended that incident definition be included in Service Level Agreements.

## 4. The IT Security Continuous Monitoring Shared Services Lifecycle

IT Security Continuous Monitoring Shared Services, as with all systems, follows a lifecycle. This section describes tasks, roles, responsibilities, assumptions, risks, security strategy, and outputs (artifacts) for each phase. Additionally, training will be addressed at a high level in the transition and operations phases. Inherent in this process is embracing Risk Management as the overarching theme which drives the security strategy. Figure 2 illustrates the IT Security Continuous Monitoring Shared Services Lifecycle phases.



**Figure 2: IT Security Continuous Monitoring Shared Services Lifecycle**

The phases encircle the IT Security Continuous Monitoring Shared Services participants who play an integral part in each of the six steps. The Agencies have a critical role in providing input to the planning, design, and implementation of this service and are the primary users during operations. The Shared Service Provider will implement the design and will provide the contracted level of service to the Agencies. Each actor may have multiple and/or different roles depending on the lifecycle phase. The relationships among these three major participants will also change depending on the phase. In some phases, additional players will contribute to phase objectives.

Each phase delivers significant program steps and milestones that are accomplished without losing respect for unique security and risk challenges. Since this is an iterative lifecycle, insertions of new technologies and services during its lifespan will be supported by the Shared Service Owner. In cases where this has been outsourced to a commercial vendor through a contract, these will be supported within the parameters and clauses of the contract. In the sections below, outputs typically needed for each phase for this type of program are listed.

However, the specific documents listed are notional depending on the System Development Lifecycle (SDLC) used, and may be combined or separated and provided by multiple entities.

The following elements of this section will describe the specifics of each phase, beginning with Phase 1, the IT Security Continuous Monitoring Shared Services Service Strategy.

#### 4.1 IT Security Continuous Monitoring Shared Services Phase 1: Service Strategy



**Figure 3: Phase 1 IT Security Continuous Monitoring Shared Services Strategy**

Figure 3 shows an overview of the Phase 1 IT Security Continuous Monitoring Shared Services strategy. IT Security Continuous Monitoring Shared Services work begins with the development of an IT Security Continuous Monitoring Shared Services strategy, led by DHS and actively supported by the Agencies participating in the IT Security Continuous Monitoring Shared Services Technical Working Group. During this strategy period, the Agencies will work with DHS on the following components of its overall IT Security Continuous Monitoring Shared Services strategy. The major steps for this phase are as follows:

1. Identify the IT Security Continuous Monitoring Shared Services Technical Working Group approach to risk management of the IT Security Continuous Monitoring Shared Services program
2. Define the IT Security Continuous Monitoring Shared Services design approach
3. Define a plan detailing how IT Security Continuous Monitoring Shared Services will secure Agency's applications
4. Define a high-level approach to test and evaluate the IT Security Continuous Monitoring Shared Services' security
5. Draft a basic framework for IT Security Continuous Monitoring Shared Services operations
6. Identify high-level conditions for improving future IT Security Continuous Monitoring services
7. Identify future conditions under which the Agency migrates away from the current IT Security Continuous Monitoring Shared Services strategy
8. Develop outlines for the critical planning documents used to design, test/evaluate, transition, operate, and improve IT Security Continuous Monitoring Shared Services

The purpose of this phase is to allow the Agencies to make an informed assessment and decision on the option of performing continuous remote monitoring of Agency premises.

#### **4.1.1 Roles**

- Agency – stakeholder and provides major input to IT Security Continuous Monitoring strategy
- FNR –strategic partner, Federal civilian lead for IT Security Continuous Monitoring, and owns IT Security Continuous Monitoring strategy

#### **4.1.2 Responsibilities**

- Agency – plans for IT Security Continuous Monitoring Shared Services, participates in developing the IT Security Continuous Monitoring Shared Services strategic framework
- FNR – provides IT Security Continuous Monitoring subject-matter expertise, lessons learned, best practices, IT Security Continuous Monitoring templates, and planning templates

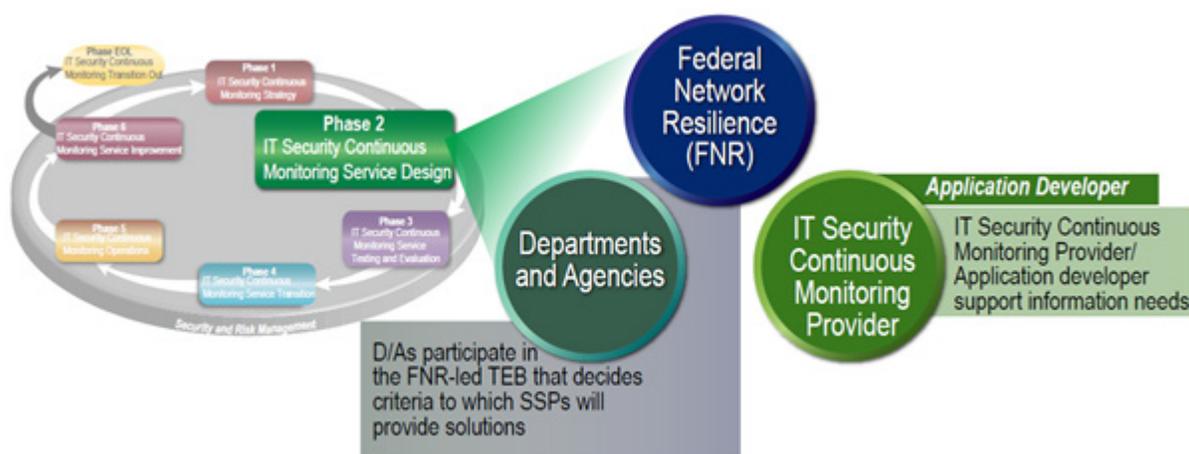
#### **4.1.3 Assumptions**

DHS and Agency are active partners in developing the Agency's IT Security Continuous Monitoring Shared Services strategy, with DHS in lead and Agency in supporting roles.

#### 4.1.4 Outputs<sup>11</sup>

- Outline of Program of Action and Milestones (POA&M)
- Outline of Design Plan
- Outline of Risk Management Plan
- Outline of Security Plan, providing for security attributes & controls, SLAs, incident-response process
- Outline of Accreditation and Authorization Plan
- Outline of Test & Evaluation Plan
- Outline of Transition Plans – Transition In and Transition Out
- Outline of Operations Plan
- Outline of Service Improvement Plan

## 4.2 IT Security Continuous Monitoring Shared Services Phase 2: IT Security Continuous Monitoring Shared Services Service Design



**Figure 4: IT Security Continuous Monitoring Shared Services Phase 2 Service Design**

Figure 4 shows an overview of the Phase 2 IT Security Continuous Monitoring Shared Services Service Design. The focus of Phase 2 is to establish the high level service design of IT Security Continuous Monitoring Shared Services. In this phase FNR and the Agency utilize the IT Security Continuous Monitoring Shared Services Strategy and information developed in Phase 1 to reach consensus on the design approach. The development of the approach will determine the service design lifecycle of IT Security Continuous Monitoring Shared Services based on Agency requirements. The phase will also determine which shared service model will be used.

<sup>11</sup> Note: The specific output documents listed for each phase are notional and depending on the SDLC used may be combined or separated and provided by multiple different entities.

The design will include sufficient flexibility to support both the Agency's size and their diverse requirements. For example, a large Agency normally has much more in-house infrastructure, resources, and expertise than some small/micro agencies. In addition, the current infrastructure and IT Security Continuous Monitoring-type capabilities already in place may vary considerably. Some Agencies' infrastructures could be hosted by a third party with SLA agreements. Agencies may also want to reuse existing infrastructure such as their sensors<sup>12</sup>. The IT Security Continuous Monitoring Shared Services design should consider reuse if feasible from both an economic and security perspective. While flexibility to meet diverse Agency needs is important to consider, the security of the system is critical, and any design decisions should be evaluated from a security risk perspective. Unique Agency scenarios like the ones identified below will be addressed on a case-by-case basis during the requirement and design activities:

- The act of scanning a device may reset it or cause it to go down
- Some devices may only be accessible via a low-bandwidth connection

Before this phase is completed, a service migration model/plan should be developed by the shared service Owner that addresses the steps and considerations for an Agency moving to IT Security Continuous Monitoring Shared Services. In addition, the acquisitions method should also be determined. While these two steps are often performed late in the design phase they can impact the decisions made in previous steps. There should be enough time allocated to this phase to allow for several iterations of the design phase before proceeding to the next phase.

The specific steps in the design phase can vary and often require working some elements in parallel or at least iterating through the key steps. The following gives a sequence of events. The most critical event to perform early is to document and prioritize the Agency requirements associated with IT Security Continuous Monitoring Shared Services.

1. Determine requirements from each Agency's perspective
2. Combine and prioritize requirements and establish consensus with key stakeholders.
3. Determine service design lifecycle and shared service model
4. Develop service migration model/plan
5. Determine acquisition method
6. Return to previous steps 3 through 5 as needed until consensus each reached.

#### **4.2.1 Roles**

The following roles are crucial to Phase 2.

- Agency – Provide input to service design by providing and explaining requirements
- FNR – Leads and coordinate service design phase
- Shared Service Providers – Provide response to requirement and propose design

---

<sup>12</sup> Note: Agencies may use their own sensor and/or other component if they meet the technical specifications under the CMaaS BPA.

## 4.2.2 Responsibilities

The following major actors are crucial to the above steps.

- Agency – Provides the requirements and obtain consensus on the key steps of this phase. Agency consensus is crucial to the success of IT Security Continuous Monitoring Shared Services
- Shared Service Provider – Coordinates input from potential Shared Service Providers on what is practical, feasible, and essential, so that the requested service meets the requirements, meets the required security elements, and is acceptable from a cost/budget perspective
  - Commercial vendors interested in being the IT Security Continuous Monitoring Shared Services Provider will be expected to respond to RFC/RFIs on IT Security Continuous Monitoring Shared Services capabilities including SLAs and security controls

## 4.2.3 Risks

- If an Agency's critical requirements are not identified at the beginning of the design phase and included in the design, then IT Security Continuous Monitoring Shared Services will not meet the objectives of the Agency. Owners: Agency
- If a Shared Service Provider cannot provide IT Security Continuous Monitoring Shared Services compliant with High-Baseline controls, then a publicly implemented IT Security Continuous Monitoring Shared Services will need to have mitigation processes and procedures in place. Owners: FedRAMP, DHS
- If the SLAs are not properly developed to meet Agency needs, then the level of service provided by a commercial Shared Service Provider might not meet the security or service delivery goals of IT Security Continuous Monitoring Shared Services. Owners: Acquisitions service provider, DHS , Agency

## 4.2.4 Security Strategy

In the design phase the security attributes, principles and SLAs described in the appendices of this document should be considered. The inclusion of these security elements in the design is essential to meet the overall security of IT Security Continuous Monitoring Shared Services and the High Confidentiality, High Integrity, and High Availability<sup>13</sup> (HHH) FedRAMP baseline controls that are required for IT Security Continuous Monitoring Shared Services.

An essential step in the design process is to be able to trace where the security elements and controls are addressed in the design. This traceability will be documented and is needed to ensure

---

<sup>13</sup> Both FedRAMP and NIST have a High Confidentiality, High Integrity, and High Availability controls. Depending on the Agency's requirements, these controls can be adopted in total or Agency-specific requirements can be specified as needed (e.g. if the application does not need to be operational 24x7 then certain High Availability controls may not be applicable).

that all the security elements and controls are included in the design and support the verification and validation steps that occur in the next phase. While all the security elements and controls are important to how IT Security Continuous Monitoring Shared Services will be audited and monitored, they have particular emphasis during the design phase since they help ensure that the other security controls are implemented and operating as expected in the operations phase.

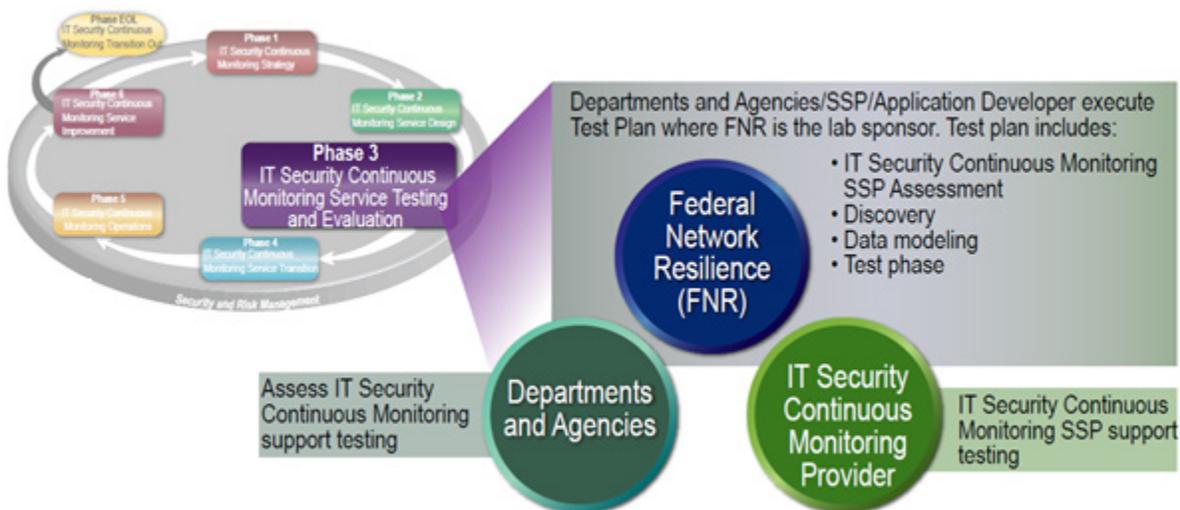
#### **4.2.5 Assumptions**

- DHS will lead the following activities for the design phase:
  - Leading all design phase activities
  - Facilitating development of IT Security Continuous Monitoring Shared Services capabilities that meet Agency requirements
  - Leading development of design phase artifacts and obtaining feedback from stakeholders
- DHS owns the following design phase risks:
  - All critical requirements are identified and prioritized early in the process
  - Ability of IT Security Continuous Monitoring Shared Services to meet HHM security requirements in a public shared environment in an economically feasible manner

#### **4.2.6 Outputs from this Phase**

- Consolidate and prioritize list of Agency requirements agreed to by stakeholders
- Selection of service design lifecycle and shared service model
- Service migration model/plan
- Acquisition method selected
- Traceability of Agency requirements and security requirements into the design so that they support the test and evaluation phase
- Any remaining issues, concerns, and risks are documented

### 4.3 IT Security Continuous Monitoring Shared Services Phase 3: Service Testing and Evaluation



**Figure 5: IT Security Continuous Monitoring Shared Services Phase 3 Service Testing and Evaluation**

Figure 5 shows an overview of the Phase 3, IT Security Continuous Monitoring Shared Services Service Testing and Evaluation. Based on the service design established and accepted by the Agency, Phase 3 begins with the creation of a test and evaluation plan for the IT Security Continuous Monitoring Shared Services design. The test and evaluation plan will provide, as appropriate, an integrated POA&M for:

- Authority to test within the established IT Security Continuous Monitoring Shared Services A&A approach
- Assessment of relevant components in the Shared Service Provider IT Security Continuous Monitoring Shared Services infrastructure
- Discovery and assessment of relevant components in the Agency's systems to be monitored
- Installation and configuration of IT Security Continuous Monitoring Shared Services components to be tested
- Data model for information to be captured and processed as part of the Agency's IT Security Continuous Monitoring Shared Services design
- Test and evaluation reports

The purpose of this phase is to validate Agency design in a structured and realistic environment, to allow for design changes prior to transition, to identify problems related to service transition, and to accelerate transition to full IT Security Continuous Monitoring Shared Services operations. Although IT Security Continuous Monitoring Shared Services itself is designed as a standardized capability, it is to be expected that each Agency's systems are unique, and may pose challenges to implementation of the standardized IT Security Continuous Monitoring Shared Services design. This test and evaluation phase is intended to identify and address those challenges before service transition begins.

### 4.3.1 Roles

- Agency – stakeholder, provides input into design and test and evaluation capability
- Shared Service Provider – stakeholder and owner of infrastructure design
- Developers of Systems under IT Security Continuous Monitoring Shared Services monitoring – SMEs needed for design or design changes
- Third Party Assessment Organization (3PAO) – FedRAMP broker

### 4.3.2 Responsibilities

- Agency – reviews and provides input into test and evaluation plan, reviews test results, accepts design as tested
- Shared Service Provider – provides routine technical support for developing the test and evaluation plan, test case development, and test execution
- Developers of Systems under IT Security Continuous Monitoring Shared Services monitoring – consultants on development of test and evaluation plan, execution of test and evaluation plan, and potentially required to assist in IT Security Continuous Monitoring Shared Services Agency-side system modifications, ensure that Agency monitoring goals are validated in the test and evaluation phase
- 3PAO – required by FedRAMP to test and assess readiness of IT Security Continuous Monitoring Shared Services Provider environment providing services to the Agency. The 3PAO<sup>14</sup> performs the following activities:
  - Create a Security Assessment Plan
  - Perform initial and periodic assessments of shared service provide security controls
  - Conduct security tests and produce a Security Assessment Report

### 4.3.3 Risks

- If there is a delay in the A&A process, then plans for implementing IT Security Continuous Monitoring Shared Services will slip. Owners: Agency, Joint Accreditation Board (JAB)
- If the assessment phase includes incomplete or inaccurate data, then the test and evaluation phase will either be invalid, or more likely fail due to lack of information relevant to a proper test. Owners: Agency and its cybersecurity contractors
- If there is a technical obstacle to implementation of one or more security controls in an Agency's system to be monitored under IT Security Continuous Monitoring Shared Services, then the test and evaluation plan schedule will probably slip, and added workloads/costs will be imposed upon the Agency and its contractor staffs. Owners: Agency and its cybersecurity contractors

---

<sup>14</sup> <http://cloud.cio.gov/fedramp/3pao>

- If there is insufficient staff technical expertise required to advance all phases of the test and evaluation, then the test and evaluation plan schedule will probably slip, and added workloads/costs will be imposed upon Agency or DHS. Owners: Agency, DHS, or Shared Service Provider
- If an Agency subsystem requires special treatment, and funding is insufficient to execute a valid test of that subsystem, then the Agency will probably experience schedule slippage and added cost in the implementation of IT Security Continuous Monitoring Shared Services. Owners: Agency
- If an Agency does not have a formal risk management board working in accordance with formal risk-management doctrine and process, then there is elevated probability of significant delays, uncoordinated response, and ineffective mitigation of specific risks that arise in the course of IT Security Continuous Monitoring Shared Services testing. Owners: Agency, Shared Service Provider

#### **4.3.4 Security Strategy**

The Security Test and Evaluation Plan is the most critical factor in mitigating Agency risk in the Test phase of implementing IT Security Continuous Monitoring Shared Services for an Agency. The plan should be designed to identify the cross-cutting risks above, shared with risk owners, and led by the Agency.

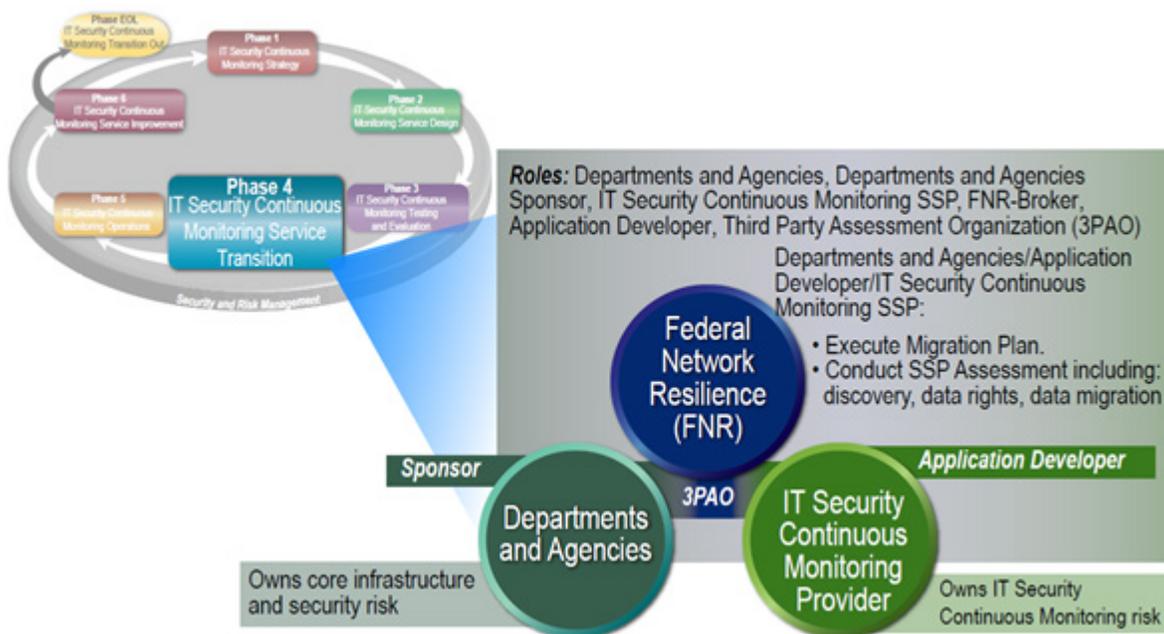
#### **4.3.5 Assumptions**

IT Security Continuous Monitoring Shared Services test facility, and facility support personnel, will be provided by the Shared Service Provider.

#### **4.3.6 Outputs**

Test and evaluation reports from this phase will be used as critical inputs to the Agency's IT Security Continuous Monitoring Shared Services Transition Plan, whose development will partially overlap test-phase activities. One of the primary objectives in the Test and Evaluation Phase is to identify and address Agency or Shared Service Provider related issues that may degrade the transition to full IT Security Continuous Monitoring Shared Services operations. Test outputs will be a key aspect to validate that key assumptions in the Transition Plan are valid. Such assumptions will vary from Agency to Agency.

## 4.4 IT Security Continuous Monitoring Shared Services Phase 4: Service Transition



**Figure 6: IT Security Continuous Monitoring Shared Services Phase 4 Service Transition**

Figure 6 shows an overview of Phase 4, IT Security Continuous Monitoring Shared Services Service Transition. Based on the service design established and accepted by the Agency in Phase 2, and additionally on results and modifications performed during Phase 3 (Testing and Evaluation), service transition will begin by finalizing the transition plan for moving the Agency's IT Security Continuous Monitoring Shared Services capability to the designated Shared Service Provider facility. Work on the transition plan will begin shortly after Phase 1 strategic planning completes, and continues in parallel with service-design phases and test and evaluation phases. By the completion of the test and evaluation phase, the transition plan should be near completion and ready for Agency sign-off. The transition plan will provide, as appropriate, an integrated POA&M for:

- Initiation of A&A documentation and required forms, within IT Security Continuous Monitoring Shared Services A&A regime
- Coordination with appropriate Agency's utilizing the shared service
- Coordination with Shared Service Provider
- Execution of final discovery of Agency's systems to be monitored
- Validation that all IT Security Continuous Monitoring Shared Services components, on Agency's and Shared Service Provider premises, are operating correctly
- Validation that Agency's system data is available and structured as described in the data model
- Validation that IT Security Continuous Monitoring reports and data are flowing to dashboards and portals per the design

- Completion of A&A forms, Agency authorization, Shared Service Provider Assumption of Full Operational Responsibility (AFOR)

The purpose of this phase is to execute a smooth transition to full IT Security Continuous Monitoring Shared Services operations, including migration of appropriate audit-log-trend data, clear delineation of data rights/ownership, availability of Agency subsystems and logs, resolution of unexpected IT Security Continuous Monitoring Shared Services problems related to transition, graceful and coordinated shutdown of obsolete monitoring/reporting capabilities, and transfer of IT Security Continuous Monitoring reporting responsibility.

#### **4.4.1 Roles**

- Agency – stakeholder and owner of systems being monitored by IT Security Continuous Monitoring Shared Services
- Shared Service Provider – stakeholder and IT Security Continuous Monitoring Shared Services infrastructure owner initiating operation of transitioned IT Security Continuous Monitoring services
- FNR – IT Security Continuous Monitoring Shared Services stakeholder and transition broker
- Developers of Agency Systems under IT Security Continuous Monitoring Shared Services monitoring – SMEs needed for design or design changes during transition
- 3PAO – FedRAMP broker

#### **4.4.2 Responsibilities**

- Agency – authorizes changes to Agency security controls to allow implementation of transition; directs Agency staff and contractors to coordinate with Shared Service Provider technical staff required for migration tasks
- Shared Service Provider – provisions Agency -specific IT Security Continuous Monitoring Shared Services infrastructure; integrates migrated Agency data into Shared Service Provider system; coordinates with Agency’s technical staff executing IT Security Continuous Monitoring Shared Services migration tasks
- FNR – broker, coordinator and transition point of escalation for Agency and Shared Service Provider
- Developers of Systems under IT Security Continuous Monitoring Shared Services monitoring – required to assist in IT Security Continuous Monitoring Shared Services Agency -side system modifications in case unexpected technical problems arise during transition
- 3PAO – required by FedRAMP to assess readiness of IT Security Continuous Monitoring Shared Services Provider environment providing services to the Agency.

### **4.4.3 Risks**

- If there is a delay in A&A issuance or other aspects of the A&A process, then Agency plans for implementing IT Security Continuous Monitoring Shared Services will slip. Owners: Agency, JAB, possibly FedRAMP
- If an Agency subsystem requires unplanned modifications during transition, and funding is insufficient to execute those modifications, then the Agency will probably experience schedule slippage and added cost in the implementation of IT Security Continuous Monitoring Shared Services. Owners: Agency
- If an Agency does not have a formal risk management board working in accordance with formal risk-management doctrine and process, then there is an elevated probability of significant delays, uncoordinated response, and ineffective mitigation of specific risks that arise in the course of IT Security Continuous Monitoring Shared Services transition. Owners: Agency, Shared Service Provider

### **4.4.4 Security Strategy**

The Transition Plan is the critical factor in mitigating Agency risk in the Migration phase of implementing IT Security Continuous Monitoring Shared Services for an Agency. The plan should be designed to identify the cross-cutting risks above, shared with risk owners, and led by the Agency with support from FNR. The Transition Plan will also identify all needed training, including how and when the training will be held.

### **4.4.5 Assumptions**

The JAB/A&A process is completed during the planned timeframes.

### **4.4.6 Outputs**

- Transition closeout and AFOR reports.
- Authority to Operate

## 4.5 IT Security Continuous Monitoring Shared Services Phase 5: IT Security Continuous Monitoring Shared Services Operations



Figure 7: IT Security Continuous Monitoring Shared Services Phase 5 Operations

Figure 7 shows an overview of the Phase 5 IT Security Continuous Monitoring Shared Services Operations. After all testing has successfully completed (Phase 3) and the service transition outlined in Phase 4 is complete, the service will go operational (Phase 5). During Phase 5, asset, configuration, and vulnerability scanning data will be transferred from the Agency to the SSP (whether the transference is based on a pull or push relationship is subject to agreement between Agency and SSP). The Agency's designated representative will access the IT Security Continuous Monitoring dashboard to review the findings and act accordingly.

### 4.5.1 Roles & Responsibilities

- IT Security Continuous Monitoring Shared Services Provider is responsible for keeping the IT Security Continuous Monitoring Shared Services scanning systems, vulnerability analysis systems and Agency dashboard up and running, including immediate fail-over to another IT Security Continuous Monitoring Shared Services Provider site should the primary IT Security Continuous Monitoring Shared Services Provider site fail. The IT Security Continuous Monitoring Shared Services Provider is also responsible for protecting the Agency's data (including PII) from disclosure to unauthorized individuals, both internal and external to the IT Security Continuous Monitoring Shared Services Provider. IT Security Continuous Monitoring Shared Services Provider is responsible for handling their own incidents, and, will notify the Agency if an incident transpired that, potentially or in fact, negatively affected the Agency's data or disclosure thereof. The IT

Security Continuous Monitoring Shared Services Provider is responsible for making IT Security Continuous Monitoring Shared Services systems available to a FedRAMP approved 3PAO to assess the IT Security Continuous Monitoring Shared Services Provider security policies, procedures and processes. The 3PAO may also perform vulnerability scans and penetration tests on the services that reside in the IT Security Continuous Monitoring Shared Services Provider's accreditation boundary.

- Agency is responsible for the infrastructure supporting the on-site scanning sensor, providing power (and applicable surge protection), network connectivity and the proper environmental control (temperature & humidity). The Agency is responsible for retrieving the vulnerability assessment data from the dashboard and then acting upon the data provided, that is, mitigating the found vulnerabilities in a judicious manner. The Agency is responsible for timely reporting of an incident to US-CERT. The Agency is responsible for taking incident response action, to the best of their ability at their site. The Agency will be responsible for authorizing their own personnel required to perform tasks related to the IT Security Continuous Monitoring Shared Services activities, including but not limited to, retrieving hardware/software asset data, vulnerability data, performing mitigation, and reporting incidents
- US Government (USG) Contracting Officer (CO) is responsible for product procurement and Engineering Change Proposals (ECPs), when applicable, and require contractual changes/modifications, schedule, cost, and program oversight. Additionally, USG CO is responsible for transition in-and-out planning.
- DHS (US-CERT and/or designated entity) is responsible for coordinating incident escalation with the USG CO on behalf of the Agency.
- 3PAO is responsible for assessing the policies, procedures and processes of the IT Security Continuous Monitoring Shared Services Provider. This may also include vulnerability scanning of the IT Security Continuous Monitoring Shared Services Provider, and, if necessary, penetration testing the IT Security Continuous Monitoring Shared Services Provider.

#### **4.5.2 Risks**

- If there is breakdown in security controls, such as the lack of protection mechanisms and controls at the IT Security Continuous Monitoring Shared Services Provider, including inadequate access, authentication and authorization controls; improper segmentation of IT Security Continuous Monitoring Shared Services virtual machines; virtual machines not hardened; data transferred in the clear; IT Security Continuous Monitoring Shared Services personnel not properly screened, IT Security Continuous Monitoring Shared Services Provider systems not kept up with patches and/or other critical maintenance requirements, then unauthorized access to Agency's data may occur. Owners: Acquisitions service provider, DHS, Agency, Shared Service Providers

- If the Configuration management plan is not implemented or if implemented, not followed, then the IT Security Continuous Monitoring Shared Services system may become insecure due to improper patching. This applies to both the IT Security Continuous Monitoring Shared Services Provider site and Agency's site(s). Owners: DHS, Agency, Shared Service Providers
- If the IT Security Continuous Monitoring Shared Services fail-over site is not correctly configured and/or not tested to prove working immediate fail-over, then the IT Security Continuous Monitoring Shared Services system may not be able to properly fail-over without losing availability of service. Owners: DHS, Agency, Shared Service Providers
- If back-ups are not tested and/or performed in a timely manner, then the system may not be able to recover from an incident without data loss. Owners: DHS, Agency, Shared Service Providers
- If incidents are not addressed correctly, then they can continue to cause damage to the system or occur on other IT Security Continuous Monitoring Shared Services systems. Owners: Acquisitions service provider, DHS, Agency, Shared Service Providers
- If IT Security Continuous Monitoring Shared Services Provider personnel fail to follow agreed upon security controls, then they may expose IT Security Continuous Monitoring Shared Services to a security incident. Owners: Acquisitions service provider, DHS, Agency, Shared Service Providers

### **4.5.3 Security Strategy**

- IT Security Continuous Monitoring Shared Services will be operated in accordance with an approved Security Plan. The Security Plan will define the operational, technical, and managerial level the controls that must be in place addressing: access controls; audit and accountability, training and awareness, security assessments, configuration management contingency planning, identification and authentication, incident response, maintenance, media protection, personnel security, physical and environmental protection, planning (includes testing), program management, risk assessment, system and communication protection, and system and information integrity
- Security SLOs should be set in the contract with the IT Security Continuous Monitoring Shared Services Provider and will translate into the IT Security Continuous Monitoring Shared Services Provider's SLA. The Shared Service Provider will provide SLO and SLA guidance based on Government Regulations, Directives, Mandates and security policies
- Additional security guidelines will be implemented such as hardening to NIST or other Government system security hardening guides. This security hardening will be applied to the machines hosting the IT Security Continuous Monitoring Shared Services applications at the IT Security Continuous Monitoring Shared Services Provider. It will be the responsibility of the IT Security Continuous Monitoring Shared Services Provider

and the Agency to adhere to the Security Plan. The security attributes (see appendix A) for this section are Protected, Governable and Trustworthy

- Configuration Management will be incorporated into the Security Plan. The Security Plan will use NIST Special Publication 800-128, “Guide for Security-Focused Configuration Management of Information Systems” for guidance. The SSP will have the responsibility to incorporate the CM guidelines into the Security Plan. The security attribute (see Appendix A) for this section is Protected.
- The Security Plan will define the fail-over site testing and evaluation; the fail-over testing will be a critical element of Phase 3 (service testing and evaluation). Additionally, the 3PAO will be called upon to periodically test and evaluate the fail-over system. The IT Security Continuous Monitoring Shared Services Provider has the responsibility for establishing and keeping the fail-over system up and running, per the Security Plan. The security attributes (see appendix A) for this section are Resilient and Usable.
- The Security Plan will define when, where, how and who will handle back-ups. The plan will include periodic testing and evaluation of back-up media. The 3PAO will periodically assess the back-up process to confirm it is being followed. The IT Security Continuous Monitoring Shared Services Provider has the responsibility of performing and managing the back-up process and procedure, per the Security Plan. The security attributes (see appendix A) for this section are Resilient and Usable.
- The IT Security Continuous Monitoring Shared Services Provider and Agencies have the responsibility of following the incident response plan as outlined in the Security Plan. The incident response plan will use NIST Special Publication 800-61 (latest revision as of the date of the IT Security Continuous Monitoring Shared Services Security Plan) as a guideline. The incident response plan will be tested during Phase 3. The security attributes (see appendix A) for this section are Resilient, Manageable, and Governable.
- It will be the Agency’s responsibility to perform, in a timely manner, mitigations required to fix found vulnerabilities. This means the Agency must be vigilant in checking the dashboard every 72 hours. Furthermore, the Agency must make a commitment to mitigate the found vulnerabilities. The security attributes (see appendix A) for this section are Resilient, Manageable and Protected.
- The 3PAO will periodically check the IT Security Continuous Monitoring Shared Services Provider to confirm the IT Security Continuous Monitoring Shared Services Provider is adhering to the Security Plan. The Agency may request a check if the Agency believes the IT Security Continuous Monitoring Shared Services Provider is not following the plan. It is the responsibility of the IT Security Continuous Monitoring Shared Services Provider to strictly follow the agreed upon Security Plan. It is the responsibility of the Agency to notify the 3PAO (or USG CO if that is how the notification procedure is established) to request a IT Security Continuous Monitoring Shared Services Provider check by the 3PAO. The security attributes (see appendix A) for this section are Manageable, Governable and Protected.

#### 4.5.4 Assumptions

- Security Plan is written prior to Phase 2 and approved by USG CO. IT Security Continuous Monitoring Shared Services Provider and Agency accept the Security Plan.
- SLOs and SLAs are well defined and accepted by the IT Security Continuous Monitoring Shared Services Provider and Agencies.
- Agency's have sufficient and trained staff to perform IT Security Continuous Monitoring Shared Services functions and infrastructure in place to support IT Security Continuous Monitoring Shared Services sensors
- IT Security Continuous Monitoring Shared Services Provider is viable and has long term prospect of staying in business
- IT Security Continuous Monitoring Shared Services Provider has competent, Outputs
- Ongoing dashboard reports that identify Agency's vulnerabilities
- Operational Lessons Learned and associated metrics to assist Phase 6 service improvements

#### 4.6 IT Security Continuous Monitoring Shared Services Phase 6: Service Improvement



**Figure 8: IT Security Continuous Monitoring Shared Services Phase 6 Service Improvement**

Figure 8 shows an overview of Phase 6, IT Security Continuous Monitoring Shared Services Service Improvement. Service Improvement is a critical maturity step for any program, as it is essential to the longevity of any Continuous Monitoring solution. Continuous monitoring by its very nature changes in several dynamic ways as time progresses, including but not limited to: new regulations, new products to monitor, new features within existing products, new reason to monitor new things, and analyzing and incorporating lessons learned. While some of these changes can be implemented by simply changing a few settings, some require major improvement of the service offering. The Service Improvement Phase serves as a defined way to transition IT Security Continuous Monitoring Shared Services from a state where all the current needs of the stakeholders are no longer met by the service, to a new state where IT Security Continuous Monitoring Shared Services, once again, is in alignment with stakeholder demands.

Monitoring of the System Performance: The key to the Service Improvement Phase is for the Agency to understand when IT Security Continuous Monitoring Shared Services is no longer fulfilling the goals it is designed to fulfill. It is important to understand what mission attributes must be met to achieve success and how these attributes will be measured so that Agencies know when it is time to move into the service improvement phase.

Transitions: Transition from the previous stage occurs when IT Security Continuous Monitoring Shared Services has reached a state, agreed upon by the Stakeholders, which requires the implementation of new features. The Transition state can be started by time (quarterly, or yearly), committee vote or by urgent situational need. In some situations, the current need outgrows the service or the service becomes outdated in concept or function. In that case, rather than continue on the lifecycle loop, the Service Improvement Phase would direct the needed improvements into Phase 7, Transition Out.

#### **4.6.1 Roles**

- Agency – the critical stakeholder for the consumption of IT Security Continuous Monitoring Shared Services
- Acquisitions Service provider – Primary contract holder/administrator

#### **4.6.2 Responsibilities**

- Agencies:
  - Remain involved in determining priorities for each improvement cycle
  - Determine when Phase 6 Service Improvement begins for each lifecycle
- Acquisitions Service provider:
  - Responsible as the central monitoring capacity for service delivery level
  - Ensure the Service Improvement capacity exists and operates in an ongoing functional manner fully engaging other Stakeholders
  - Ensure Critical Mission Attributes set in the SLA are monitored and reported when stakeholder set thresholds are not met.
  - Ensure there is a capacity to measure and track industry changes in IT Security Continuous Monitoring Shared Services as well as changes in Stakeholder demand

#### **4.6.3 Risks**

- If the Agencies and the Shared Service Provider fail to monitor Critical Mission Attributes or inadvertently measure the wrong attributes for IT Security Continuous Monitoring Shared Services set by the Stakeholders in the SLA, then the mission will be negatively impacted and the IT Security Continuous Monitoring Shared Services will quickly become dated and less functional than desired by Agency Stakeholders. Owners: Acquisitions service provider, DHS, Agency, Shared Service Providers
- If the Agency and the Shared Service Provider fail to adequately monitor the environment for critical changes to the continuous monitoring landscape, then that failure

will adversely impact the protection of the IT Security Continuous Monitoring Shared Services system and the systems it is designed to protect. While this may seem like a risk that is shared with the vendor providing the IT Security Continuous Monitoring Shared Services shared service, the core risk remains with FNR and the Agencies using IT Security Continuous Monitoring Shared Services. The mission impact is such that a change will occur that puts the existing “as is” service into an unknown vulnerable state, resulting in potential data release which could cause cascading impacts to the agencies that use the system. Owners: Acquisitions service provider, DHS, Agency, Shared Service Providers

### 4.6.4 Security Strategy

When considering service improvements it is best practice to revisit the original analysis. As introduced in section one and elaborated on in Appendix A, the security attributes and principles that were considered in this SECONOPS should be reviewed and updated to reflect the current environment and challenges.

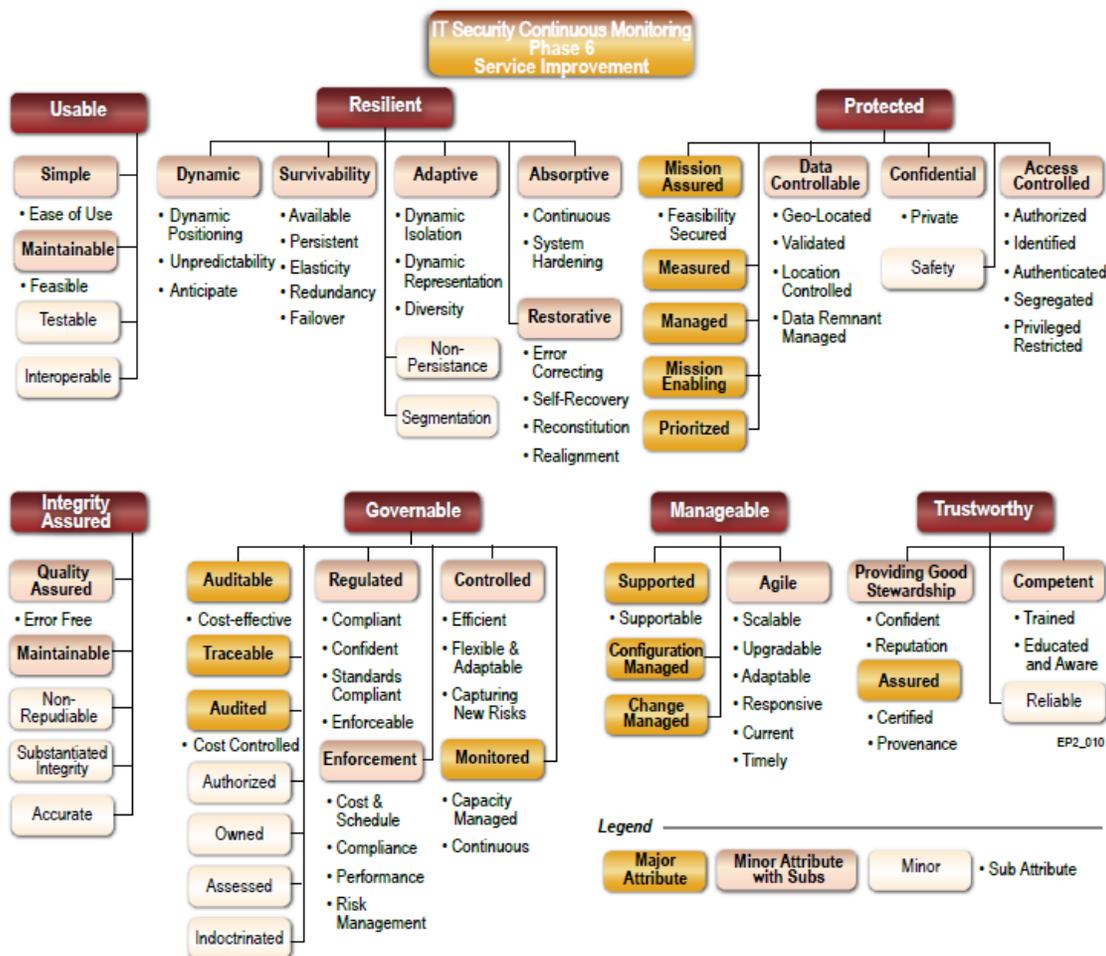
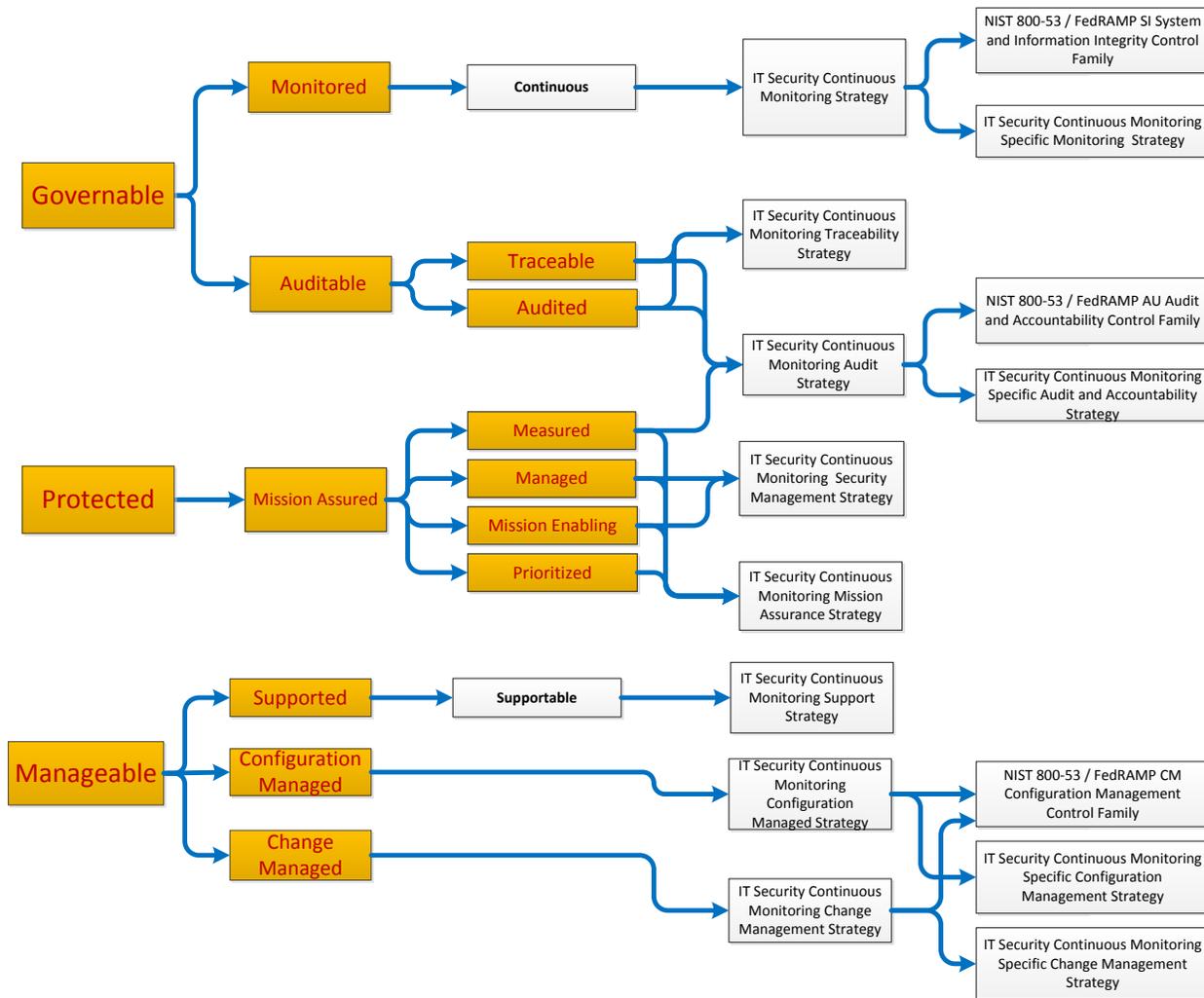


Figure 9: IT Security Continuous Monitoring Shared Services Phase 6 Security Attributes

Figure 9 shows notional Security Attributes that should be considered during the service improvement phase. To ensure that the stakeholder needs are addressed, this phase requires participation on the part of the Agency Stakeholders.

Security Strategy for this Phase: Figure 10 shows (highlighted in yellow) the major security attributes associated with Phase 6.



**Figure 10: IT Security Continuous Monitoring Shared Services Service Improvement Security Attributes**

Phase 6 is primarily a programmatic effort by DHS in conjunction with the major stakeholders to continuously monitor the state of the environment the IT Security Continuous Monitoring Shared Services program operates in, looking for improvements or major changes, as well as to continuously monitor the desired service level of the existing IT Security Continuous Monitoring Shared Services system as designated by major stakeholders of IT Security Continuous Monitoring Shared Services. The success of the service improvement phase is closely tied to the long term success and maturity of the IT Security Continuous Monitoring Shared Services program as a whole. To accomplish these goals and mitigate the risks associated with this phase, the outlined Mission Security Attributes, shown in Figure 10, are primarily designed to achieve Protection, Mission Assurance, Manageability, and program Governance.

#### 4.6.5 Assumptions

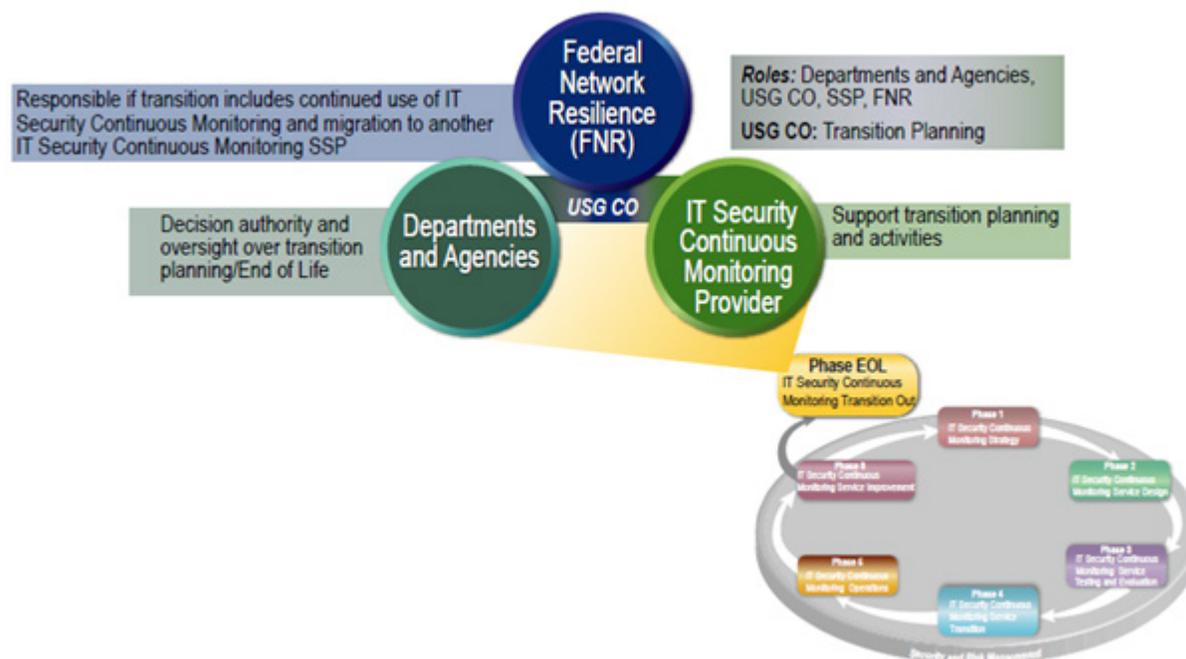
DHS, in coordination with its acquisitions service provider, will be responsible for the Service Improvement Phase even if DHS outsources the implementation of the actual Phase - they would remain in charge of oversight and engage Agencies as to when, how often, and by what measure this phase is initiated within the defined parameters of contract clauses.

#### 4.6.6 Outputs

The Service Improvement Phase has two major output paths:

- Prioritized service improvement requirements to be designed in the next iteration of Phase 1
- Direction to move to Phase 7, Transition Out, in the case where stakeholder demands in Phase 6 exceed the capacity for the existing IT Security Continuous Monitoring Shared Services program to change

### 4.7 IT Security Continuous Monitoring Shared Services Phase 7: End of Life: IT Security Continuous Monitoring Shared Services Transition Out



**Figure 11: IT Security Continuous Monitoring Shared Services Phase End-of-Life (EOL): Transition Out**

Figure 11 shows an overview of Phase 7, IT Security Continuous Monitoring Shared Services Transition Out. The End of Life (EOL) for IT Security Continuous Monitoring Shared Services could take many forms and paths. For example, new technologies might emerge that revolutionize the mechanism to combat cyber and other attacks; new approaches on offering services or solutions may emerge, making a more traditional or different deployment approach of greater value; or threats may appear that necessitate a revolutionary approach to defend. In many

cases, this phase will parallel the early phases for the replacing system. A critical step in this phase is to understand and integrate the business needs driving to the new system. Critical milestones in this phase are synchronized with milestones from the actual project designated to replace this system.

#### **4.7.1 Roles**

- Agency – stakeholder and decision authority
- IT Security Continuous Monitoring Shared Services Provider – actor
- DHS –transition broker
- Acquisitions service provider CO – stakeholder

#### **4.7.2 Responsibilities**

- Agency – provides inputs to the shared service owner for the replacement system and oversight over transition planning/End of Life
- Shared Service Provider – recommends pioneering technologies as a replacement; support the transition to the new system
- DHS –leads the closedown of the IT Security Continuous Monitoring Shared Services into a new system. A new organization could serve in DHS’s role
- Acquisitions service provider CO – provides the governance on the existing contract closing down and for the new project startup and operations. Also responsible for transition planning along with FNR

#### **4.7.3 Risks**

- If there are not adequate resources to maintain IT Security Continuous Monitoring Shared Services, then new threats could go undetected possibly increasing the effectiveness of attacks. Owners: Acquisitions service provider, DHS, Agencies
- If the replacement system is not deployed on time, then extra resources may be required to maintain IT Security Continuous Monitoring Shared Services. Owners: Acquisitions service provider, DHS, Agencies
- If IT Security Continuous Monitoring Shared Services is not replaced before it becomes obsolete, then IT Security Continuous Monitoring Shared Services might not be able to handle the threats to the system and ability to manage threats, becomes less effective. Owners: Acquisitions service provider, DHS, Agencies

#### **4.7.4 Security Strategy**

Continuous monitoring is performed on the IT Security Continuous Monitoring Shared Services infrastructure through the end of life. This will help to maintain an effective barrier to attacks on the system. System Support and Confirmation/Change Management continues on the system until operations cease to maintain IT Security Continuous Monitoring Shared Services Manageability. Full (if not elevated) Governance ensures that the system receives adequate levels of support and is a key mitigation for the first risk identified above. As discussed in D.7

Termination or Transfer of Service, it is critical to ensure that all Agencies' data is appropriately handled and all copies the Shared Service Provider has are destroyed using approved procedures.

#### **4.7.5 Assumptions**

Adequate time and resources are provided to ensure a smooth transition to the new system. IT Security Continuous Monitoring Shared Services provides a minimally acceptable environment to provide Agency adequate continuous monitoring.

#### **4.7.6 Outputs**

IT Security Continuous Monitoring Shared Services smoothly shuts down.

## **5. Portal (Location, Protection, and Availability)**

The term “portal” represents a generic user facing user interface that represents the IT Security Continuous Monitoring dashboard or other portals that may be needed to support IT Security Continuous Monitoring Shared Services.

Section 2 introduced the IT Security Continuous Monitoring Dashboard and additional notational portals that may be needed to provide IT Security Continuous Monitoring Shared Services information. In either case, the communication between the IT Security Continuous Monitoring Shared Services and the portal will be protected using a secure method, such as a Federal Information Processing Standard (FIPS) -certified encrypted communications path. The availability requirements for the portal should be consistent with those for IT Security Continuous Monitoring Shared Services. Redundant, protected communication paths should be considered to prevent the communication link between IT Security Continuous Monitoring Shared Services and the portal from being a single point of failure impacting all the Agencies. If either IT Security Continuous Monitoring Shared Services, or the portal, fails-over to another site, communication between the portal and IT Security Continuous Monitoring Shared Services will be reestablished in a timely manner after the failover.

## 6. References, Acronyms, and Abbreviations

### 6.1 References

Table 5 lists the relevant industry standards used to prepare this document. Table 6 lists the Government-provided documents and standards used by the IT Security Continuous Monitoring Shared Services team. Table 7 lists the specific Project documents and standards used by the team.

**Table 5: Standards Used**

Document and Version	Date
NIST SP 800-123, "Guide to General Server Security"	July 2008
NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"	December 2011
NIST SP 800-146, "Cloud Computing Synopsis and Recommendations"	May 2012
NIST SP 800-125, "Guide to Security for Full Virtualization Technologies"	January 2011
FIPS Publication 140-2, "Security Requirements for Cryptographic Modules"	December 2002
NIST SP 800-61, "Computer Security Incident Handling" Guide	August 2012, July 2012
NIST SP 800-57, "Recommendation for Key Management"	May 2014
"Virtualization Security: Protecting Virtualized Environments" by David Shackelford, Sybex publishers, ISBN-10: 1118288122	November 2012
NIST SP 500-292, "Cloud Computing Reference Architecture"	September 2011
Joint publication from CIO Council and Chief Acquisitions Officers Council, in coordination with Federal Cloud Compliance Committee "Creating Effective Cloud Computing Contracts for the Federal Government"	February 24, 2012
NIST Interagency Report 7622 "Supply Chain Risk Management Practices for Federal Information Systems"	November 2012
Federal Emergency Management Agency's (FEMA's) Federal Preparedness Circular (FPC) 65	June 2004
NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information Systems"	August 2011
NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," as amended	May 2013
Cloud Security Alliance, "Shared Service Level Agreement Standardization Guidelines"	June 24, 2014
Department of Defense (DoD) Architecture Framework, v 2.0.2	August 2012
MEMORANDUM FOR CHIEF INFORMATION OFFICERS "Security Authorization of Information Systems in Cloud Computing Environments" From Steven VanRoekel Federal, CIO	December 8, 2011
MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES M-15-01 "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices" From Steven VanRoekel, Federal CIO	October 3, 2014
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES M-14-03 "Enhancing the Security of Federal Information and Information Systems" From Sylvia M. Burwell	November 18, 2013

Document and Version	Date
“Federal Information Technology Shared Services Strategy”, Executive Office of the President of the United States	May 2, 2012
“Federal Shared Services Implementation Guide” CIO Council	April 16, 2013
“Guide to Understanding FedRAMP” Version 2.0	June 6, 2014
NIST SP 800-88, “Guidelines for Media Sanitization ”	September 2006

**Table 6: Government Documents Used**

Document and Version	Date
Office of Cybersecurity and Communications (CS&S) Style Guide	April 2014
FNR Master Acronym List (FNR_PEG_STD_MasterAcronymList_F1.0)	September 2014

**Table 7: IT Security Continuous Monitoring/IT Security Continuous Monitoring Shared Services Documents Used**

Document and Version	Date
Concept of Operations (CONOPS) for IT Security Continuous Monitoring Version 1.0	March 11, 201
GSC-QF0B-BPA-14-32865 CMaaS TO2B RFQ 2014.08.18;	August 18, 2004

## 6.2 Acronyms and Abbreviations

All acronyms and abbreviations in this document are defined at first occurrence. Refer to the FNR Master Acronym List for a compilation of all acronyms and abbreviations used within DHS FNR, including those used in this document. The FNR Master Acronym List, located on the FNR SharePoint, is updated periodically and approved for use by the FNR Process Engineering Group (PEG).

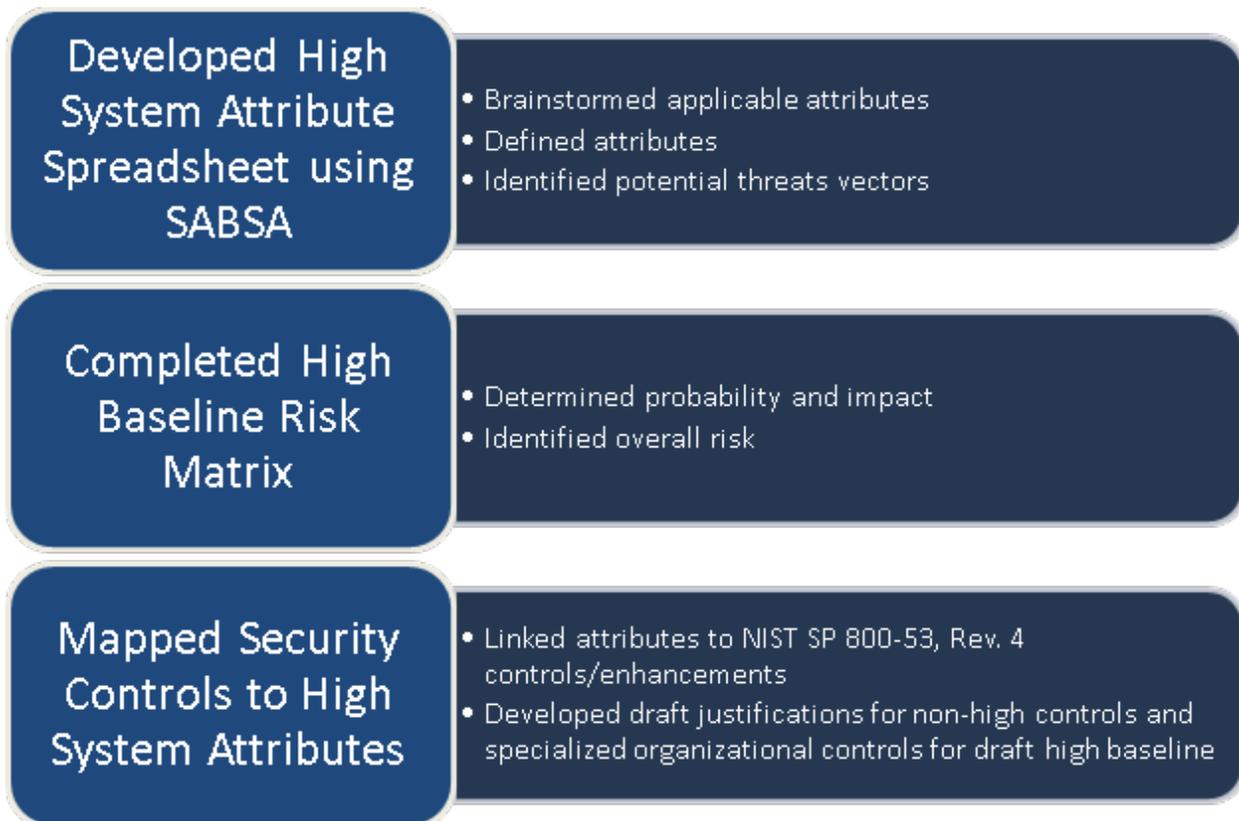
## **Appendix A: Mission Attributes and Mission Assurance Principles**

Establishing mission attributes and assurance principles for IT Security Continuous Monitoring Shared Services provides an essential foundation to communicate the contextual and conceptual principles on which the service will be established. The attributes provide a common framework for a stakeholder to determine and accept the base principles on which the SECONOPS and the IT Security Continuous Monitoring Shared Services Lifecycle will be based.

An evaluation by DHS of IT Security Continuous Monitoring Shared Services has determined that the system requires HHM FIPS 199 Security Classification for Confidentiality, Integrity and Availability (CIA). The SECONOPS is not intended to be a comprehensive list of all security controls; rather it addresses the primary security attributes developed by using a Sherwood Applied Business Security Architecture (SABSA) approach. SABSA is fundamentally used as a framework to understand the mission objectives at each layer of an organization down to the asset level. SABSA helps to assure the project security is both complete and traceable to the mission. The SABSA process can be seen throughout the SECONOPS lifecycle phases as the stakeholders answer the “six big questions” (i.e., Who, What, Where, Why, How, and When). SABSA was used as a framework to understand the mission objectives at each layer of an organization down to the asset level and to assist with assuring that project security was complete and traceable to broad mission objectives of the federal government. Once the attributes were identified, definitions were developed, potential threat vectors and risks for each attribute were identified, the risk for each attribute were then evaluated and finally the attributes were linked to the NIST 800-53 controls. In addition to this top-down approach, an independent bottom-up approach was performed, as illustrated in Figure 12. The bottom-up approach started with the NIST 800-53 R4 Security Controls Catalog as a baseline and leveraged the following sources:

- FedRAMP Moderate Security Controls Baseline
- NIST Cloud Computing Security Working Group’s Draft High Baseline for FedRAMP
- DISA Enterprise Cloud Services Broker (ECSB) Level 5 (H-H-X) Baseline
- DoD 8500.02 IA Controls.

The bottom-up approach took in to consideration the leveraged sources when determining candidate security controls for a shared services environment with an overall security categorization of “High.” Once the top-down and bottom-up approaches were complete, the approaches were compared; inconsistencies were resolved, resulting in a draft High baseline for a shared services environment. In Appendix A, Mission Attributes and Mission Assurance Principles, Figure 13 contains the SABSA Attribute Chart and then defines attribute definitions.



**Figure 12: Process for Developing Shared Service High Baseline**

This appendix contains the Attribute Chart shown in Figure 13 and the definitions for each attribute.

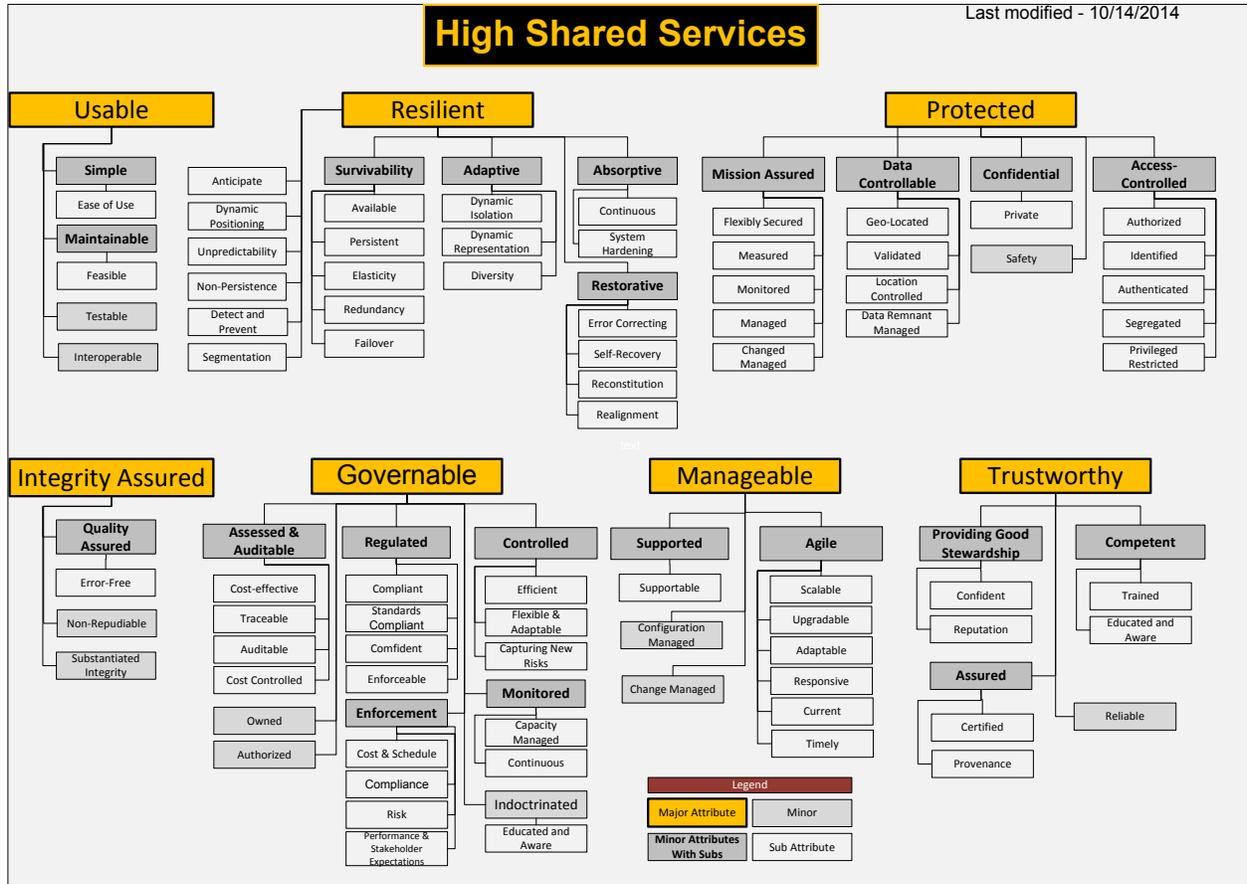


Figure 13: High Security Baseline Attributes for a Shared Service

When developing security attributes, threats against the following were considered: Technology, People, Processes, and Environment. For each of these categories the following threat types were considered:

- Technology
  - Technology and infrastructure
  - Applications and services
  - Facilities and operating environment
  - Information security
  - Supply chain
- People
  - Behavioral
  - Criminal and illicit acts
  - Ethics
  - Health and safety
- Processes
  - Business strategy
  - Risk management framework
  - Cultural
  - Project management
  - Public relations
  - Governance
  - Legal and regulatory compliance
  - Product liability
  - Human Resources
- Environment
  - Climate, weather, environment, and geology
  - Geo-political
  - Terrorism, war ,and similar events

## **A.1 Protected Attributes/Principles**

Protected: Assets (something or someone) should be defended against abuse:

- Confidential: The system preserves authorized restrictions on information access and disclosure, including means for protecting personally identifiable/proprietary information
  - Privacy: The ability to protect Personally Identifiable Information (PII)
- Data Controllable: The assurance that data is handled in a manner that is in congruence with stakeholder expectations concerning location, segregation, and access
  - Geo-located (Attribution): The assurance that something or someone is where they claim to be
  - Validated: The assurance that something or someone is what they claim they are
  - Location Controlled: In the correct place to access what it is to access (could be data, physical, or logical)
  - Data Remnant Managed: The assurance that data removed from any form of media is not left behind

- Access-Controlled: The access to information and functions within the system are managed in accordance with authorized privileges
  - Privileged Restriction: To restrict privileges required to use cyber resources based on types, degrees of criticality, and trust
    - Weakest Link: The most fragile and/or vulnerable element within a system that is the easiest to exploit
    - Least Functionality: The system is configured to provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services
    - Least Privilege: To limit the level of authorization to only those needed to perform required job functions (i.e., only those involved in the management, analysis, and/or mitigation of vulnerabilities need to see the asset and vulnerability data in the portal.
    - Potential Authorized Roles: Agency System Administrators (SAs), Agency Information Assurance (IA)/(IT) Manager
    - Need to Know: The security principle that limits access to data or resources to those required to complete a job function by an individual within the organization (i.e., each Agency will only have access to their own data, not the data of any other Agency). Potential Authorized Roles: Agency SAs, Agency IA/IT Manager
    - Separation of Duties: A security principle to break a business process into separate functions and assign to different people (i.e., to make a change to IT Security Continuous Monitoring Shared Services should require approval from the appropriate Configuration Control Board (CCB) and at least one IT Security Continuous Monitoring Shared Services SA). Requiring two IT Security Continuous Monitoring Shared Services SAs would be preferred but may not be practical to implement and enforce
    - Least Common Mechanism: A security principle that prevents a mechanism used to access resources from not being shared
    - Complete Mediation: A security principle that ensures authorization is checked on every request for a resource. Authentication and Authorization between scanning component and IT Security Continuous Monitoring Shared Services should be validated every instance of use. Also, Authentication and Authorization between IT Security Continuous Monitoring Shared Services users and the portal should be validated each time it is used and not cached. This principle is particularly important if the design provides any opportunity for a Man-In-The-Middle (MITM) attack (i.e., client side, cookie-based caching is particularly vulnerable to an MITM attack if complete mediation is not employed)

- Authorized: The system should allow only those actions that have been explicitly authorized
  - Authorization: The system confirms the user is approved to use the system and/or view specific data
  - Multifactor Authentication: Applying multiple authentication means to verify a user is who they say they are by employing a minimum combination of two (can be more) authentication techniques: Something you know, something you have, something you are, and/or someplace you are (either Internet Protocol (IP) address or Global Positioning System (GPS) coordinates)
  - Limit Unsuccessful Login Attempts: A threshold that states after a predetermined number of unsuccessful login attempts, the system is locked
  - Role Based Access Control (RBAC): A collection of permissions, with all users receiving permissions only through the roles to which they are assigned, or through roles they inherit through the role hierarchy
  - Attribute Based Access Control: A rule-based approach to access control
  - Single-Sign-On (SSO): An access control method where access to multiple systems is allowed by the user only providing his credentials once. One of the more secure methods for implementing SSO is through the use of an X.509 digital certificate. Authentication to IT Security Continuous Monitoring Shared Services and the portal will be through a Personal Identity Verification (PIV) card
- Identified: Each entity that will be granted access to system resources and each object that is itself a system resource should be uniquely identified (named) such that there can never be confusion as to which entity or object is being referenced
  - Identification: To assert or claim credentialing to an authentication system
- Authenticated: Every party claiming a unique identity (e.g., a claimant) should be subject to a procedure that verifies that the party is indeed the authentic owner of the claimed identity
  - Authentication: The system confirms a user is who they say they are
- Segregated: The system should segregate actions, data, and processes from unauthorized or unrelated action, data, and processes
- Mission Assured: The system is configured and assured in a way that allows for the mission to be achieved correctly and identify when the achievement of the mission is off track
  - Flexibly Secured: Security can be provided as the system changes. The system should continue to be secure as the system scales, expands, and changes

- Measured: The performance of the system against a variety of desirable performance targets should be measured so as to provide feedback information to support the management and control process
  - Managed: The act of managing the system and processes
  - Change Managed: Changes to the system should be properly managed so that the impact of every change is evaluated and the changes are approved in advance of being implemented
- Safety: The assurance of being free from harm or damage (this would include people, data, and infrastructure)
  - Fail Safe: The system design prevents or mitigates unsafe consequences of a system's failure
  - Fail Secure: Should the system fail, the security of the system remains intact as before the failure

## A.2 Resilient Attributes/Principles

Resilient: A resilient system absorbs breaches by operating at reduced performance, deflects damage by operating at known higher risk of failure, and recovers itself through adaptation or subsystem restoration.

- Absorptive: The system continues to operate within normal performance limits while unanticipated events hit the system
  - Continuous/High Availability: To maximize the duration and viability of essential mission functions without interruption
  - System Hardening: The system continues to function when a component fails or encounters an error/ flaw
- Survivability: The capability to withstand a negative event, without significant impairment to the mission, at a potentially degraded performance
  - Available: The proportion of time a system is in a functioning condition from a user perspective
  - Persistent: To ensure information, services, and connectivity are preserved on system failure or breach
  - Elasticity: The degree to which a system is able to adapt to workload conditions
  - Redundancy: The elimination of single points of failure by providing duplicative or alternate methods for completing a needed function/capability of the system
  - Failover: The ability to switch one or more components of a system to a redundant component or system
- Adaptive: The systems change configuration to maintain operations
  - Dynamic Isolation: The ability to contain a threat and segregate it from legitimate/authorized information
  - Dynamic Representation: Different depiction/configurations
  - Diversity: To leverage the designed set of heterogeneous technology (e.g., hardware, software, protocols, firmware)
- Restorative: The ability of a system to be returned to a known, good state
  - Error Correcting: The ability to detect and repair issues impacting the integrity of the data or system behavior
  - Self-Recovery: The ability to restore system capability without human intervention
  - Reconstitution: The ability of the system to be restored to its original state
  - Realignment: The ability to use the system's diversity to reestablish system capabilities
- Anticipate: The ability to proactively counter changes to the system that could impact the mission
- Dynamic Positioning: The use of distributed processing and automated relocation of critical assets and sensors to thwart attacks

- Unpredictability: To automatically and dynamically make system configuration changes so they appear random but do not impact system functionality or the mission
- Non-persistent: To retain information, services, and connectivity for a limited time
- Segmentation: Separate (logically or physically) components to limit damage
- Detect and Prevent: The ability to identify a threat and counter it prior to it compromising the mission
- Defense in Depth: A combination of people, process and technology working seamlessly creating, deploying, and maintaining multiple layers of cyber defense for a system

### **A.3 Usable Attributes/Principles**

Usable: The system functions at the level for which it was designed.

- Simple: The system should be as simple as possible, since complexity only adds further risk
  - Ease of Use: The system should be designed so that the user interface follows human factors' best practices to facilitate efficiency and productivity for activities required to accomplish the mission
    - Economy of Mechanism: The security mechanism should be as simple as possible and easy to understand. Simplicity generally leads to less errors and components that are easier to test and/or verify
- Maintainable: From the perspective of the staff maintaining the system, the system should be capable of being fixed, updated, or enhanced without disruption to the mission
  - Feasible: The actions required to achieve this should be feasible within the normal operational conditions of the system
- Testable: System capabilities will be verifiable
- Interoperable: The agreed to interfaces (standards) will be in place and should maintain linkages with other versions for a period of time

### **A.4 Integrity Assured Attributes/Principles**

Integrity-Assured: The integrity of the mission, including its assets and information, should be protected so that it does not suffer unauthorized modification, duplication, or deletion.

- Quality Assured: There should be a means to ensure the system is operating as expected and that all the various controls are correctly implemented and operated in support of the mission
  - Error-Free: The system should operate without producing errors. If errors occur, they should be handled and logged so that data is not corrupted or can be recovered from a backup in a timely fashion
- Non-Reputable: The actions in support of the mission should guarantee attribution to source and content

- Digital Signatures: The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, assurance of data integrity, and signatory non-repudiation
  - Signatory: The entity that generates a digital signature on data using a private key
  - Signature Generation: The process of using a digital signature algorithm and a private key to generate a digital signature on data
  - Signature Verification: The process of using a digital signature algorithm and a public key to verify a digital signature on data
  - Verifier: The entity that verifies the authenticity of a digital signature using a public key
  - Private Key/Private Signature Key: A cryptographic key used with an asymmetric (public key) cryptographic algorithm that is associated with a public key. The private key is uniquely associated with the owner and is not made public. This key is used to compute a digital signature that may be verified using the corresponding public key
  - Public Key/Public Signature Verification Key: A cryptographic key used with an asymmetric (public key) cryptographic algorithm that is associated with a private key. The public key is associated with an owner and may be made public. In the case of digital signatures, the public key is used to verify a digital signature signed using the corresponding private key
- Substantiated Integrity: To ascertain that critical services, information stores, etc., have not been corrupted

## A.5 Governable Attributes/Principles

Governable: The management and oversight that provides effective authority and timely situational awareness of risk.

- Assessed and Auditable: To evaluate that a system and subsystems supports specific missions to a standard and acceptable level of risk. There are sufficient controls and measures on the system to support an audit
  - Cost effective: The design, acquisition, implementation, and operation of the system should be achieved at a cost the business finds acceptable when judged against the benefits derived
  - Auditable: The actions of all parties having authorized access to the system and the complete chain of events and outcomes resulting from these actions should be recorded so that this history can be reviewed. The audit records should provide an appropriate level of detail in accordance with business needs
  - Cost-controlled: The clear identification of the major cost drivers in the system, in a way that allows for cost performance tracking in all lifecycle phases

- Traceable schedule: The clear identification of the work breakdown structure, including all key Agency management milestones, mapped explicitly to an integrated program schedule at a level of detail permitting industry-standard, critical-path, and Monte-Carlo analytics, thus yielding a human-independent method for assessing schedule risk in all lifecycle phases
- Traceable performance: The focus on system performance, clear identification of operations metrics relevant to mission effectiveness, and to cost metrics that are a function of Service-level metrics
- Traceable mission capabilities: The focus on mission capability and identification of Agency mission capabilities that will be affected by system/subsystem capability
- Traceable mission risk: The focus on mission risk, explicit connection of operations metrics with risk to Agency mission capability, and to Agency "crown jewels"
- Regulated: Specific standards identified and rules/guidelines/exceptions are defined, documented, signed, and promulgated
  - Compliant: The system should comply with all applicable regulations, laws, contracts, policies, and mandatory standards, both internal and external
  - Standards Compliant: The system should be designed, implemented, and operated to comply with appropriate technical and operational standards
  - Confident: The system should behave in such a way as to safeguard confidence placed in the organization by customers, suppliers, shareholders, regulators, financiers, the marketplace, and the general public
  - Enforceable: The system should be designed, implemented, and operated such that all applicable contracts, policies, regulations, and laws can be enforced by the system
- Controlled: The effective exercise of authority to direct and prioritize efficient operations of the system, modify operations to meet changing requirements, or adapt operations to other environmental forces, be they financial, security-driven, or risk driven
  - Efficient: The system should deliver the target services with optimum efficiency, avoiding wastage of resources
  - Flexible and Adaptable: The system should be flexible and adaptable to meet new business requirements as they emerge
  - Capturing new risks: New risks emerge overtime. The system management and operational environment should provide a means to identify and assess new risks (new threats, new impacts, or new vulnerabilities)
- Monitored: The effective use of metrics to track and report compliance, cost, schedule, performance, and mission risks to meet mission objectives
  - Capacity-managed: The capacity to monitor the system and evaluate against current and forecast demand

- Continuous: The system should offer “continuous service.” The exact definition of this phrase will always be subject to an SLA
- Enforcement: The use of continuous monitoring to exercise control over the relevant technologies, processes, and personnel, to ensure that risk to Agency mission and information security is effectively managed; secondarily, use of standards, cost, and schedule monitoring will trigger enforcement/mitigation action designed to ensure the Agency 's credibility is not threatened by overruns or compliance failure
  - Compliance: The effective use of metrics, to track and report desired outcome with applicable regulation and capability-capacity targets
  - Cost and Schedule: The effective use of metrics, to periodically track and report identified resources and time
  - Performance and Stakeholder Expectations: The effective use of metrics to confirm mission support
  - Risk: The effective use of metrics to monitor threats to the mission in near-real-time
- Authorized: The system has been approved for operation
- Owned: The entities responsible for all aspects of the system, including data (mission sponsor, execution, CIO, etc.)
- Indoctrinated: Education and awareness requires that the knowledge, skills, abilities, and position descriptions/roles are defined. Once the roles are defined the personnel receive or have the required training, testing, and certifications for their current role

## A.6 Manageable Attributes/Principles

Manageable: The ability to control and operate (update, monitor, diagnose, respond, report, and audit) the shared service efficiently and correctly

- Agile: The ability to quickly implement changes and adapt to conditions
  - Scalable: The system should be scalable to the size of the user community, data storage requirements, processing throughput, etc., that might emerge over the lifetime of the system
  - Upgradable: The system should be capable of being upgraded with ease to incorporate new releases of hardware and software
  - Adaptable: Changes and processes can be made easily as technology progresses
  - Responsiveness: To react within a satisfactory period of time that meets expectations
  - Current: The information provided to users should be current and kept up-to-date, within a range that has been pre-agreed as being applicable for the service being delivered
  - Timely: The information is delivered or made accessible to the user at the appropriate time or within the appropriate time period

- Open Design: The design is based on standards and open architecture that allow ease of integration of new technologies
- Supported: The people, tools, and processes are in place to assist as needed
- Supportable: The system can efficiently be updated and fixed as needed
- Configuration Managed: The people, tools, processes, and training are in place to control the assets
- Change Managed: The people, tools, processes, and training are in place to control modification before implementation

## **A.7 Trustworthy Attributes/Principles**

Trustworthy: To behave in a predictable manner while protecting against a wide range of potential threats.

- Providing Good Data Stewardship: The wise use and care of provided resources. In a shared environment, the data will be protected/managed appropriately
  - Confident: The system should behave in such a way as to safeguard confidence placed in the organization by the customers, suppliers, shareholders, regulators, financiers, marketplace, and general public
  - Reputation: The system should behave in such a way as to safeguard the business reputation of the organization
- Assured: There should be a means to provide assurance that the system is operating as expected and that all the various controls are correctly implemented and operated
  - Provenance (origination): Supply Chain - chronology of the ownership, custody, or location of an object's history
  - Certified: The systems are confirmed to have adequate controls
- Competent: The people associated with the system have the appropriate training, knowledge, and ability to execute
  - Trained: The personnel have obtained the necessary training or knowledge required to support the mission
  - Educated and Aware: The user community should be educated and trained so that they can embrace the security culture and so as to have sufficient user awareness of security issues that behavior of users is compliant with security policies
- Reliable: The system consistently meets user expectations for its adequate performance (in a generic sense, not just speed)

## Appendix B: Service Level Agreements (SLAs)

This appendix includes common SLOs that relate to the Shared Service Provider's performance and the related aspects of the interface between the shared service customer and the Shared Service Provider. Before discussing the shared SLOs, commonly used SLA terms<sup>15</sup> are defined below in Table 8.

**Table 8: Commonly Used SLA Terms**

Definition	Description
Application Programming Interface (API)	The collection of invocation methods and associated parameters used by a certain (part of) Shared Service Provider or software component to request actions from and otherwise interact with another Shared Service Provider or software component
Auditability	The capability of supporting a systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled
Availability	The property of being accessible and usable upon demand by an authorized entity <sup>16</sup>
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. <sup>17</sup>
Shared infrastructure	The collection of hardware, software, and other related goods and resources that enable the provision of the Shared Service Provider's service
Shared service	One or more capabilities offered via shared computing invoked using a defined interface
Shared service consumer	A party that is in a business relationship for the purpose of using Shared Service Providers.
Shared service consumer data	A class of data objects under the control, by legal or other reasons, of the Shared Service Provider customer that were input to the shared service, or resulted from exercising the capabilities of the Shared Service Provider by or on behalf of the Shared Service Provider customer via the published interface of the shared service. An example of legal controls is copyright.
Shared service provider derived data	A class of data objects under the Shared Service Provider's control derived as a result of interaction with the Shared Service Provider by the Shared Service Provider customer. Shared Service Provider derived data includes log data containing records of who used the service, at what times, and which functions and types of data were involved. The data can also include information about the numbers of authorized users and their identities and can include any configuration or customization data where the Shared Service Provider has such configuration and customization capabilities
Shared service provider SLO	A target for a given attribute of a Shared Service Provider that can be expressed quantitatively or qualitatively

<sup>15</sup> Cloud Security Alliance, "Shared Service Level Agreement Standardization Guidelines," June 24, 2014

<sup>16</sup> Adapted from NIST 800-146

<sup>17</sup> Adapted from NIST 800-145

Definition	Description
Shared service provider	A party which makes shared services available
Shared service provider data	A class of data objects, specific to the operation of the Shared Service Provider, under the control of the Shared Service Provider. Provider data includes, but is not limited to, resource configuration and utilization information, shared service specific Virtual Machine (VM) storage and network resource allocations, overall data center configuration and utilization, physical and virtual resource failure rates, and operational costs
Shared service provider user	Natural person, or entity acting on their behalf, associated with a Shared Service Provider customer that uses shared services. Examples of such entities include devices and applications
Shared SLA lifecycle	SLA lifecycle (e.g., assessment, negotiation, contracting, operation, amendment, escalation and termination, and other arrangements and matters)
Shared SLAs	The documented agreement between the Shared Service Provider and Shared Service Provider customer that identifies services and Shared Service Provider SLOs
Cryptographic key management	The management of cryptographic keys in a cryptosystem, including the generation, exchange, storage, use, and replacement of keys, as well as cryptographic protocol. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols
Data	Information in any form, nature, or structure, that can be created, uploaded, inserted in, collected, or derived from or with Shared Service Providers and/or shared computing, including without limitation proprietary and non-proprietary information, confidential and non-confidential information, non-personal and personal information, as well as other human-readable or machine-readable information
Data controller	The natural or legal person, public authority, Agency, or any other body which alone or jointly with others determines the purposes and means of the processing of data
Data format	One or more layouts in which the data is in one or more phases of its data lifecycle
Data integrity	The property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit. <sup>18</sup>
Data intervenability	The capability of a Shared Service Provider to support the shared service customer in facilitating exercise of the rights of data subjects. <b>NOTE:</b> Rights of data subjects include without limitation access, rectification, and erasure of the personal data of the data subject. This also includes the objection to processing of the personal data when it is not carried out in compliance with the applicable legal requirements
Data lifecycle	The handling of data that commonly includes six (6) phases: (1) create/derive, (2) store, (3) use/process, (4) share, (5) archive, and (6) destroy
Data location	The geographic location(s) where data may be stored or otherwise processed by the Shared Service Provider
Data portability	Ability to easily transfer data from one system to another without being required to re-enter data

<sup>18</sup> Adapted from NIST 800-33

Definition	Description
Data processor	A natural or legal person, public authority, Agency, or any other body that processes personal data on behalf of the Data controller
Data protection	The employment of technical, organizational, and legal measures to achieve the goals of data security (confidentiality, integrity, and availability), transparency, intervenability and portability, as well as compliance with the relevant legal framework
Data subject	An identified or identifiable natural person; being an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity
Hybrid cloud	The deployment model of shared computing using at least two shared deployment models
Identity assurance	The ability of a relying party to determine, with some level of certainty, that a claim to a particular identity made by some entity can be trusted to actually be the claimant's true, accurate, and correct identity
Incident notification and transparency	The notifications and transparency about incidents under the SLA that may be required as per (a) mandatory law, regulation and/or legislation.
Information security	The preservation of confidentiality, integrity, and availability of information
Infrastructure as a Service (IaaS)	The capability provided to the Shared Service Provider customer is to provision processing, storage, networks, and other fundamental computing resources where the Shared Service Provider customer is able to deploy and run arbitrary software, which can include operating systems and applications. The Shared Service Provider customer does not manage or control the underlying shared infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)
Incident management	The processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents
Metric	A metric is a defined measurement method and measurement scale used in relation to a quantitative SLO
Personal data	Any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity.
Platform as a Service (PaaS)	The capability provided to the Shared Service Provider customer to deploy onto the shared infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the Shared Service Provider. The Shared Service Provider customer does not manage or control the underlying shared infrastructure including network, servers, operating systems, or storage, but has control over the deployed
Private cloud	The shared infrastructure is provisioned for exclusive use by a single organization comprising multiple Shared Service Provider customers (e.g., business units). The cloud may be owned, managed, and operated by the organization, a third party, or some combination of them, and may exist on or off-premises

Definition	Description
Processing of personal data	Any operation or set of operations that is performed on Personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, or erasure or destruction
Public cloud	The shared infrastructure is provisioned for open use by the general public. The cloud may be owned, managed, and operated by a business, academic, or Government organization, or some combination of them, and exists on-premises of the Shared Service Provider and/or its suppliers
Records Management	The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved in the records life cycle -- creation, maintenance and use, and disposition. Records management provides for the adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations <sup>19</sup>
Response time	Time interval between a Shared Service Provider customer initiated event (stimulus) and a Shared Service Provider initiated event in response to that stimulus
Representational State Transfer (REST)	A software architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system
Reversibility	The process for Shared Service Provider customers to retrieve their Shared Service Provider customer data and application artifacts and for the Shared Service Provider to delete all Shared Service Provider customer data as well as contractually specified Shared Service Provider derived data after an agreed upon period
Sensitive data	Any classified, personal, proprietary or confidential information or data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with Shared Service Providers and/or shared computing whose access, use, disclosure or processing is subject to restriction either by applicable law or contract
Software as a Service (SaaS)	The capability provided to the Shared Service Provider customer to use the Shared Service Provider provider's applications running on a shared infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The Shared Service Provider customer does not manage or control the underlying shared infrastructure, which includes network, servers, operating systems, storage, or individual application capabilities, with the possible exception of limited user-specific application configuration settings
Temporary data	The data or a data set created during the operation of the shared service that becomes unused after a predefined period of time
Vulnerability	A weakness of an asset or group of assets (e.g., software or hardware related) that can be exploited by one or more threats

<sup>19</sup> <http://www.archives.gov/records-mgmt/faqs/>

Definition	Description
Anything-as-a-Service (XaaS)	A collective term of diverse but re-useable components, including without limitation: infrastructure, platforms, data, software, middleware, hardware, or other goods, made available as a service with some kind of use of shared computing

## B.1 Common SLOs

The common SLOs described below need to be examined and evaluated for inclusion in the SLA for the Shared Service Provider:

- **AVAILABILITY:** Availability is usually covered by certification at a general level. Availability is a key SLO since it describes whether the shared service can actually be used, and is typically necessary to specify numeric values for availability to make meaningful statements useful for Shared Service Provider customers.

The question of what "usable" means is a complex matter that depends on the Shared Service Provider concerned. A service can be up and available but perform so poorly that it is effectively unusable. Similarly, the service can be up but respond with errors for valid requests. It can be valuable for the SLA to provide clear information on these aspects of service availability. Table 9 shows the availability SLOs.

**Table 9: Availability SLOs**

SLO	Description
Level of uptime (often termed "availability")	The time in a defined period the service was available, over the total possible available time, expressed as a percentage. <sup>20</sup> Some shared services specify that the service will be unavailable for specified periods for maintenance. It is common for the stated level of uptime to exclude these maintenance periods. In this case, Uptime = Total Possible Available Time – (Total Downtime – Maintenance Downtime)
Percentage of successful requests	The number of requests processed by the service without an error over the total number of submitted requests, expressed as a percentage
Percentage of timely service provisioning requests	The number of service provisioning requests completed within a defined time period over the total number of service provisioning requests, expressed as a percentage. Provisioning of shared services may vary greatly depending on the type of service being considered – from storage provisioning to user account provisioning. It is thus expected that this SLO will need to be tailored to the particular service being considered

<sup>20</sup> Uptime can be defined as the Total Possible Available Time – (Downtime – Allowable Downtime). The Total Possible Available Time is the number of total minutes, hours, seconds in the measurement period, usually a billing month. Allowable Downtime accounts for scheduled maintenance and any other element carved out in the agreement

- **RESPONSE TIME:** Response time is the time interval between a Shared Service Provider customer-initiated event (stimulus) and a Shared Service Provider-initiated event in response to that stimulus. The response time of SLOs can vary depending on the point at which the customer stimulus is measured. For example, the measurement may start from when the customer initiates the stimulus on their device, or it may start from the point where when the request from the customer arrives at the Shared Service Provider's endpoint – the difference being the network transit time, which may be outside the control of the Shared Service Provider. Similarly, the point at which the response is measured can vary.

Response time can be a highly significant aspect of the user experience of a shared service. For some requests, response times greater than a given threshold are regarded as unacceptable and can make the shared service effectively unusable. Rarely are response times dealt with directly by certifications. Furthermore, response times can vary depending on the nature of the request or type of service being considered.

A factor that should be considered is that many shared services support multiple operations and that it is likely that the response time will differ for the different operations. As a result, response time SLOs should clearly state which operation(s) are concerned. Table 10 show the response time SLOs.

**Table 10: Response Time SLOs**

<b>SLO</b>	<b>Description</b>
Average response time	Refers to the statistical mean over a set of Shared Service Provider response time observations for a particular form of request
Maximum response time	Refers to the maximum response time target for a given particular form of request

- **CAPACITY:** Capacity is the maximum amount of some property of a shared service. It is often an important value for Shared Service Provider customers to know when using a shared service.

The relevant properties vary depending on the capabilities offered by the Shared Service Provider, which is often the case that multiple capacities are relevant for a given shared service.

Capacities are rarely the subject of certification and will be stated clearly in the SLA for a shared service. Table 11 shows the Capacity SLOs. **NOTE:** Capacity SLOs refer to the capacities as seen by an individual shared service customer and do not reflect the overall capacities supported by the Shared Service Provider. It is commonly the case that the customer can change the capacity limits for their shared service(s) by requesting a change in their subscription.

**Table 11: Capacity SLOs**

<b>SLO</b>	<b>Description</b>
Number of simultaneous connections	Refers to the maximum number of separate connections to the shared service at one time
Number of simultaneous shared service users	Refers to a target for the maximum number of separate shared service customer users that can be using the shared service at one time
Maximum resource capacity	Refers to the maximum amount of a given resource available to an instance of the shared service for a particular shared service customer. Example resources include data storage, memory, and number of Central Processing Unit (CPU) cores
Service throughput	Refers to the minimum number of specified requests that can be processed by the shared service in a stated time period. (e.g., Requests per minute)

- **CAPABILITY INDICATORS:** Capability indicators are SLOs that promise specific functionality relating to the shared service.

Capabilities can be essential to the use of the shared service from the perspective of the shared service customer. Table 12 shows the capability indicator SLOs.

**Table 12: Capability Indicator SLOs**

SLO	Description
External connectivity	Specifies capabilities of the shared service to connect to systems and services external to the shared service The systems and services involved may be other shared services or may be outside shared computing (e.g., in-house customer systems)

- **SUPPORT:** Support is an interface made available by the Shared Service Provider to handle issues and queries raised by the shared service customer

Support capabilities may be required by certification, but the details are typically not covered by certification and will instead be described by SLOs. Table 13 shows the support SLOs.

**Table 13: Support SLOs**

SLO	Description
Support hours	Specifies the hours during which the Shared Service Provider provides a shared service customer support interface that accepts general inquiries and requests from the shared service customer
Support responsiveness	Specifies the maximum time the Shared Service Provider will take to acknowledge a shared service customer inquiry or request. It is typical for responsiveness to vary depending on a severity level, which is attached to the customer request, with a shorter response time associated with higher severity levels
Resolution time	Refers to the target resolution time for customer requests (i.e., the time taken to complete any necessary actions as a result of the request). This target time can vary depending on the severity level of the customer request, with shorter times attached to requests of higher severity

- **REVERSIBILITY/TERMINATION PROCESS:** The reversibility/termination process takes place when a shared service customer or a Shared Service Provider elects to terminate the agreement. The termination process includes a series of steps that enable the customer to retrieve their shared service customer data within a stated period of time before the Shared Service Provider deletes the shared service customer data from the provider's systems (including backup copies, which may be done possibly on a different schedule). The Shared Service Provider can potentially delete or aggregate any shared

service derived data (limited to derived data related to operations) that relates to the customer and their use of the shared service, although such deletion may be limited in scope.

Certification may require a well-defined termination process but does not typically define aspects such as the time periods involved. Table 14 shows the reversibility/termination process SLOs.

**Table 14: Reversibility/Termination Process SLOs**

<b>SLO</b>	<b>Description</b>
Data retrieval period	Specifies the length of time the customer can retrieve a copy of their shared service customer data from the shared service
Data retention period	Refers to the length of time the Shared Service Provider will retain backup copies of the shared service customer data during the termination process (in case of problems with the retrieval process or for legal purposes). This period may be subject to legal or regulatory requirements, which can place lower or upper bounds on the length of time the provider can retain copies of shared service customer data
Residual data retention	Refers to a description of any data relating to the shared service customer that is retained after the end of the termination process, typically this will be shared service derived data, which could be subject to regulatory controls

- **SERVICE RELIABILITY:** Service reliability is the property of a shared service to perform its function correctly and without failure, typically over some period of time. This category is usually related to the security controls implementing business continuity management and disaster recovery in frameworks such as FPC 65. Allowable downtime, which accounts for scheduled maintenance and any other element carved out in the agreement, should be taken into account for this SLO.

**NOTE:** Reliability also covers the capability of the shared service to attend to failures and avoid loss of service or loss of data in the face of such failures.

Reliability is sometimes covered by certification, but the target for reliability should be stated so the shared service customer can assess whether the particular shared service meets their business requirements. Some data management SLOs can be relevant to reliability. Table 15 shows the service reliability SLOs.

**Table 15: Service Reliability SLOs**

<b>SLO</b>	<b>Description</b>
Level of redundancy	Describes the level of redundancy of the shared service supply chain, possibly taking into account the percentage of components or services that have failover mechanisms.

SLO	Description
	Redundancy also varies on the type of shared service provided (Infrastructure as a Service (IaaS) versus Software as a Service (SaaS) for example)
Service reliability	Describes the ability of the shared service to perform its function correctly and without failure over a defined period

- **AUTHENTICATION and AUTHORIZATION:** Authentication is the verification of the claimed identity of an entity (typically for shared computing the entity is a shared service user). Authorization is the process of verifying an entity has permission to access and use a particular resource based on predefined user privileges. Authentication and authorization are key elements of information security that apply to the use of shared services.

Certification generally validates that authentication and authorization mechanisms are in place for a system, but do not in general provide details of how those mechanisms are provided, which can be essential information for the shared service customer. Table 16 shows the authentication and authorization SLOs.

**Table 16: Authentication and Authorization SLOs**

SLO	Description
User authentication and identity assurance level	Measures the Level of Assurance (LoA) of the mechanism used to authenticate a user accessing a resource. The LoA can be based on relevant standards (e.g., NIST SP 800-63 (Electronic Authentication Guidelines))
Authentication	Specifies the available authentication mechanisms supported by the Shared Service Provider on its offered shared services. In some cases the customer may need to analyze, along with the Shared Service Provider, those mechanisms allowing interoperability among their authentication schemes (e.g., cross-certification in the case of digital certificate-based authentication)
Mean time required to revoke user access	The arithmetic average of the times required to revoke user access to the shared service on request over a specified period of time
User access storage protection	Describes the mechanisms used to protect shared service user access credentials
Third party authentication support	Specifies whether third party authentication is supported by the shared service and defines which technologies can be used for third party authentication <sup>21</sup>

- **CRYPTOGRAPHY:** Cryptography is a discipline that embodies principles, means, and methods for the transformation of data to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use (also known by the term

<sup>21</sup> Other authentication SLOs may become less relevant if authentication is performed by a third party

encryption). Simply, it is turning plain readable text into unreadable text (by the human eye).

While many certification approaches require the use of data encryption in a variety of circumstances, there are many encryption methods in use and these methods vary in their strength and their cost - either in terms of performance or of the necessary processing power to use them. It is necessary for the SLA to describe specifics relating to encryption methods for the shared service customer to evaluate a shared service fully. since few certifications require the use of specific encryption methods. Table 17 shows the cryptography SLOs.

**Table 17: Cryptography SLOs**

SLO	Description
Cryptographic brute force resistance	Expresses the strength of a cryptographic protection applied to a resource based on its key length and algorithm (i.e., using FIPS encryption security levels <sup>22</sup> ). Instead of using key lengths alone, which are not always directly comparable from one algorithm to another, this normalizing scale allows comparison of the strengths of different types of cryptographic algorithms
Key access control policy	Describes how strongly a cryptographic key is protected from access when it is used to provide security to the shared service (or assets within the shared service)
Cryptographic hardware module protection level	Describes the level of protection afforded to cryptographic operations in the shared service through the use of cryptographic hardware modules

- INCIDENT MANAGEMENT and REPORTING:** An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. Information security incident management involves the processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

How information security incidents are handled by a Shared Service Provider is of great concern to shared service customers since an information security incident relating to the shared service is also an information security incident for the shared service customer. Table 18 shows the incident management and reporting SLOs.

<sup>22</sup> FIPS PUB 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001, including change notices

**Table 18: Incident Management and Reporting SLOs**

<b>SLO</b>	<b>Description</b>
Percentage of timely incident reports	Describes the defined incidents to the shared service reported to the customer in a timely fashion. This is represented as a percentage by the number of defined incidents reported within a predefined time limit after discovery, over the total number of defined incidents to the shared service that are reported within a predefined period (e.g., month, week, year, etc.)
Percentage of timely incident responses	Describes the defined incidents assessed and acknowledged by the Shared Service Provider in a timely fashion. This is represented as a percentage by the number of defined incidents assessed and acknowledged by the Shared Service Provider within a predefined time limit after discovery, over the total number of defined incidents to the shared service within a predefined period (e.g., month, week, year, etc.)
Percentage of timely incident resolutions	Describes the percentage of defined incidents against the shared service resolved within a predefined time limit after discovery

- **LOGGING and MONITORING:** Logging is the recording of data related to the operation and use of a shared service. Monitoring means determining the status of one or more parameters of a shared service. Logging and monitoring are ordinarily the responsibility of the Shared Service Provider.

Log file entries are important to shared service customers when analyzing incidents (e.g., security breaches and service failures) as well as in monitoring customer day-to-day use of the service. It is necessary for there to be SLOs relating to logging and to fully describe the shared service and its related capabilities. Table 19 shows the logging and monitoring SLOs.

**Table 19: Logging and Monitoring SLOs**

<b>SLO</b>	<b>Description</b>
Logging parameters	Describes the parameters captured in the shared service log files
Log access availability	Describes log file entries the shared service customer has access to
Log retention period	Describes the period of time during which logs are available for analysis (e.g., the period of time that log files are available for use by the shared service customer)
Audit Log Access	Audit logs will be accessed through the SSP portal. The audit log data will be updated every 72 hours.

- **AUDITING and SECURITY VERIFICATION:** Auditing is the systematic, independent, and documented process for obtaining audit evidence about a shared service and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The audit evidence required and the audit criteria are usually determined by the audit

scheme or certification scheme used to perform the audit. Certification is one of many ways to address audits.

Audits are a means by which the Shared Service Provider can offer independent evidence that a shared service meets particular criteria of interest to the shared service customer – aiming to increase trust in the shared service. Table 20 shows the auditing and security verification SLOs.

**Table 20: Auditing and Security Verification SLOs**

SLO	Description
Certifications applicable	Refers to a list of certifications held by the Shared Service Provider for a shared service, including the certifying body, the expiration date of each certification, and the renewal period

- **VULNERABILITY MANAGEMENT:** Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

Effective management of vulnerabilities ensures that information about technical vulnerabilities of information systems is obtained in a timely fashion, evaluated for organizational exposure, and addressed to mitigate the associated risk. Table 21 shows the vulnerability management SLOs.

**Table 21: Vulnerability Management SLOs**

SLO	Description
Percentage of timely vulnerability corrections	Describes the number of vulnerability corrections performed by the Shared Service Provider, and represented as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the shared service reported within a predefined period (e.g., month, week, year)
Percentage of timely vulnerability reports	Describes the number of vulnerability reports by the Shared Service Provider to the shared service customer, and represented as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the shared service reported within a predefined period (e.g., month, week, year)
Reports of vulnerability corrections	A description of the mechanism by which the Shared Service Provider informs the customer of vulnerability corrections applied to the provider's systems, including the frequency of the reports

SLO	Description
False positive	A false positive occurs when a vulnerability scan states there is vulnerability, but in reality there is no vulnerability. False positives occurring more than 10% of the total True Positive vulnerabilities found is unacceptable and root-cause analysis will be performed immediately to determine how and why false positives are occurring. False positives found will be reported via the SSP Metrics section of the SSP portal and will be clearly available to the Agency. Additionally, false positive root-cause analysis findings and their associated resolution will be documented on the Shared Service Portal.

- **SERVICE CHANGES:** Shared services may change from time to time. Examples of service changes include changes to functionality, changes to the service's interfaces, and the application of software updates. Change to a particular service can be reflected in the SLA or in another contractual document.

Shared service customers need a reasonable notification period before changes to a shared service take effect so that they can plan appropriately. Table 22 shows the service changes SLOs.

**Table 22: Service Changes SLOs**

SLO	Description
Shared service customer data use by provider	Describes stated policy for any intended use of shared service customer data
Shared service derived data use	Describes what derived data is created by the Shared Service Provider from shared service customer data, the intended uses for the derived data, and what rights the shared service customer has to inspect the derived data

- **DATA CLASSIFICATION:** Data classification is a description of the data classes associated with the shared service:
  - Shared service customer data
  - Shared Service Provider data
  - Shared service derived data

Shared service customer data is a class of data objects under the control of the shared service customer. Shared service customer data includes data input into the shared service by the shared service customer and the results of the shared service customer's use of the shared service, unless the master service agreement specifically defines a different scope.

The following SLOs, shown in Table 23, contain a specific list of data uses (provider and derived) that can be applied to compare different Shared Service Providers' offers in a concrete manner. This information is usually difficult to deduce in such a specific and

concrete way from relevant security/data protection certifications. Customers should use this information to make informed decisions about their choice of Shared Service Provider (i.e., are the Shared Service Provider’s listed “customer data uses” compliant with my requirements?)

**Table 23: Data Classification SLOs**

SLO	Description
Shared service customer data use by the provider	Describes stated policy for any intended use of shared service customer data
Shared service derived data use	Describes what derived data is created by the Shared Service Provider from shared service customer data, the intended uses for the derived data, and what rights the shared service customer has to inspect the derived data

- **DATA MIRRORING, BACKUP, and RESTORE:** This SLO category deals with the actual mechanisms used to guarantee the customer data is available (online or offline) in case of failures forbidding access to it. The mechanisms falling under the scope of this SLO are divided in two widely-used categories: (1) data mirroring, and (2) backup/restore.

Widely used security certification contains specific security controls implemented to avoid data loss. However, in many cases the information that can be extracted from those certifications rarely contains the basic measurements that can be used by the shared service customer to assess/monitor if the implemented data security controls actually fulfill their requirements. In particular, refer to SLOs in the following areas:

- The timeliness of the mirroring mechanisms that might be directly related with the geographical location of the Shared Service Provider’s data centers
- Concrete details related to the frequency and method used by the Shared Service Provider’s backup and recovery mechanism(s)

Proposed SLOs allow customers to fine-tune their risk assessment and business continuity procedures. The SLOs can assist the shared service customer in putting in place Recovery Point Objective (RPO) and Recovery Time Objective (RTO) when using the shared service.

RPO is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. In particular, RPO affects data redundancy and backup. A small RPO suggests mirrored storage of both transient and persistent data, while a larger window allows for a periodic backup approach. Shared service customers should determine their acceptable RPO for each

shared service they use and ensure the shared service providers and their own disaster recovery plans meet their objectives.

RTO is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Shared services can be critical components of business processes. Shared services customers will determine the RTO for each of their shared service dependent business processes and likewise determine whether the shared service providers and the shared service customers' disaster recovery plans are sufficient. Table 24 shows the data mirroring, backup, and restore SLOs.

**Table 24: Data Mirroring, Backup, and Restore SLOs**

SLO	Description
Data Mirroring Latency	Refers to the difference between the time data is placed on primary storage and the time the same data is placed on mirrored storage
Data Backup Method	Refers to a list of method(s) used to backup shared service customer data
Data Backup Frequency	Refers to the period of time between complete backups of shared service customer data
Backup Retention Time	Refers to the period of time a given backup is available for use in data restoration
Backup Generations	Refers to the number of backup generations available for use in data restoration
Maximum Data Restoration Time	Refers to the committed time taken to restore shared service customer data from a backup
Percentage of Successful Data Restorations	Refers to the committed success rate for data restorations, expressed as the number of data restorations performed for the customer without errors over the total number of data restorations, expressed as a percentage

- **DATA LIFECYCLE:** The following list of SLOs is related to the efficiency and effectiveness of the provider's data lifecycle practices, with a particular focus on the practices and mechanisms for data handling and deletion.

The following list of SLOs provides information related with the assurance and timeliness associated with the deletion mechanism. Furthermore, it may be of interest for the shared service customer to be able to retrieve data after a deletion request has been posted and to have SLOs associated with data retrieval.

Shared service customers are expected to use the list of SLOs, as shown in Table 25, to decide on the choice of available shared storage mechanisms offered by the Shared Service Provider.

**Table 25: Data Lifecycle SLOs**

SLO	Description
Data deletion type	Describes the quality of data deletion, ranging from “weak” deletion where only the reference to the data is removed, to “strong” sanitization techniques to ensure that deleted data cannot be easily recovered <sup>23</sup>
Percentage of timely effective deletions	Refers to the number of shared service customer data deletion requests completed within a predefined time limit over the total number of deletion requests, expressed as a percentage
Percentage of tested storage retrievability	Refers to the amount of shared service customer data that has been verified to be retrievable during the measurement period, after the data has been deleted

- **DATA PORTABILITY:** The following list of SLOs, as shown in Table 26, is related to the Shared Service Provider capabilities to export data, so it can still be used by the customer (i.e., in the event of terminating the contract).

In related security controls frameworks and certifications the implementation of data portability controls usually focuses on the specification of applicable Shared Service Provider policies, which makes it difficult (and sometimes impossible) for shared service customers to extract the specific indicators related with available formats, interfaces, and transfer rates. The following list of SLOs focuses on these three basic aspects of the Shared Service Provider data portability features, which can be used by the customer (i.e., to negotiate the technical features associated with the provider’s termination process).

**Table 26: Data Portability SLOs**

SLO	Description
Data portability format	Specifies the electronic format(s) shared service customer data can be transferred to/accessed from the shared service
Data portability interface	Specifies the mechanisms that can be used to transfer shared service customer data to and from the shared service. This specification potentially includes the specification of transport protocols and the specification of APIs or of any other mechanism supported
Data transfer rate	Refers to the minimum rate at which shared service customer data can be transferred to/from the shared service using the mechanism(s) stated in the data interface

- **CODES OF CONDUCT, STANDARDS, AND CERTIFICATION MECHANISMS:** The shared service customer, as data controller, will accept responsibility for abiding by the applicable data protection legislation. Notably, the shared service customer has an

<sup>23</sup> Refer to “NIST SP 800-88: Guidelines for Media Sanitization,” September 2006

obligation to assess the lawfulness of the processing of personal data in the shared service and to select a Shared Service Provider that facilitates compliance with the applicable legislation.

In this regard, the Shared Service Provider should make available all necessary information, also in adherence to the principle of transparency, as described hereinafter. Such information includes information that may assist in the assessment of the service, (e.g., data protection codes of conduct, standards or certification schemes the service complies with). Table 27 shows the SLOs for codes of conduct, standards, and certification mechanisms.

**Table 27: Codes of Conduct, Standards, and Certification Mechanisms SLOs**

SLO	Description
Applicable data protection codes of conduct, standards, certifications	A list of the data protection codes of conduct, standards, and certification mechanisms the service complies with

- **PURPOSE SPECIFICATION:** The principle of purpose specification and limitation requires that personal data will be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. Therefore, the purposes of the processing will be determined, prior to the collection of personal data, by the data controller, who will also inform the data subject thereof.

When the data controller decides to process the data in the Shared Service Provider's system, they will ensure that personal data are not (illegally) processed for further purposes by the Shared Service Provider, or one of his/her subcontractors.

In general, the Shared Service Provider may not process personal data, pursuant to the service agreement with its customer, for its own purposes, without the express permission of the customer. Otherwise, a Shared Service Provider that processes customer personal data for its own purposes outside an explicit mandate from its customer (i.e., to perform market analysis or scientific analysis, to profile data subjects, or to improve direct marketing, all for its own account), will qualify as a data controller in its own right and will fulfill all relevant obligations.

It is therefore important that the list of processing purposes (if any), which are beyond those requested by the customer, is defined. Table 28 shows the SLOs for purpose specifications.

**Table 28: Purpose Specifications SLOs**

SLO	Description
Processing purposes	A list of processing purposes (if any) beyond those requested by the customer acting as a controller

- **DATA MINIMIZATION:** The shared service customer is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for specific purposes In Accordance With (IAW) Government laws, regulations directives mandates and defined through contract clauses.

Furthermore, temporary data can be created during the operation of the shared service, and may not be immediately deleted once the data becomes unusable for technical reasons. Periodic checks should ensure that such temporary data is effectively deleted after a predefined period. Temporary data is defined as but not limited to, data that can be stored in memory (e.g. buffers) or in temporary files such as auto save files or files used to export data from applications that can be used as machine readable data to other applications (e.g metadata)

- The contract between the shared service customer and provider will include clear provisions for the erasure of personal data IAW Government laws, regulations directives and mandates.
- Furthermore, since personal data may be kept redundantly on different servers at different locations, it will be ensured that each instance of them is erased irretrievably (e.g., previous versions, temporary files, etc.) IAW Government laws, regulations directives mandates and contract clauses

The following SLOs, as shown in Table 29, complement these indications by translating them in a measurable objective that applies the data minimization principle in the course of the service.

**Table 29: Data Minimization SLOs**

SLO	Description
Temporary data retention period	The maximum period of time that temporary data is retained after identification that the temporary data is unused
Shared service customer data retention period	The maximum period of time that shared service customer data is retained before destruction by the Shared Service Provider and after acknowledgment of a request to delete the data or termination of the contract

- **USE, RETENTION, and DISCLOSURE LIMITATION:** The Shared Service Provider, in its capacity as data processor, should inform the customer, in the most expedient time possible under the circumstances, of any legally binding request for which the provider is compelled to disclose the personal data by a law enforcement or Governmental authority, unless otherwise prohibited, such as a legal prohibition to preserve the confidentiality of an investigation.

Besides the above mentioned obligation to inform the customer, the following SLOs, as shown in Table 30, aim to quantify the disclosures to law enforcement authorities over a period of time; this may also permit the customer to compare multiple offerings by different providers.

**Table 30: Use, Retention, and Disclosure Limitation**

SLO	Description
Number of customer data law enforcement disclosures	Refers to the number of personal data disclosures to law enforcement authorities over a predefined period of time (applicable only if the communication of such disclosures is permitted by law)
Number of personal data disclosure notifications	Refers to the number of personal data disclosures to law enforcement authorities actually notified to the customer over a predefined period of time (applicable only if the communication of such disclosures is permitted by law)

- **OPENESS, TRANSPARENCY, and NOTICE:** Only if the provider informs the customer about all relevant issues, the shared service customer is capable of fulfilling its obligation as data controller to assess the lawfulness of the processing of personal data in the cloud. Moreover, the Shared Service Provider will make available the information that enable the customer to provide the data subjects with an adequate notice about the processing of their personal data, as required by law.

Notably, transparency in the shared service means it is necessary for the shared service customer to be made aware of Shared Service Providers' subcontractors contributing to the provision of the respective shared service.

The processing of certain special categories of data may require compliance with specific statutes and regulatory provisions, which may not be covered by standards or certifications schemes of general application. Therefore, it should be specified within the service agreement the possible special categories of data that the service is suitable for. Table 31 shows the SLOs for openness, transparency, and notice.

**Table 31: Openness, Transparency, and Notice**

SLO	Description
List of tier 1 subcontractors	Refers to the Shared Service Provider's subcontractors involved in the processing of the shared service customer data
Special categories of data	Refers to the list of the specific categories of personal data (if any) (e.g., health-related, financial data, or otherwise sensitive data) the shared service is suitable for processing, according to applicable standards or regulations

- **ACCOUNTABILITY:** In the field of data protection, accountability often takes a broad meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure data protection principles have been implemented.

In this context, IT accountability is particularly important in order to investigate personal data breaches; to this end, the shared platform should provide reliable monitoring and logging mechanisms, as described in the relevant sections of these guidelines.

Moreover, Shared Service Providers should provide documentary evidence of appropriate and effective measures designed to deliver the outcomes of the data protection principles (e.g., procedures designed to ensure the identification of all data processing operations, to respond to access requests, designation of data protection officers, etc.). In addition, shared service customers, as data controllers, should ensure they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority, upon request.

The Shared Service Provider will notify the shared service customer in the event of a data breach that affects the customer data. To this end, the Shared Service Provider will implement a data breach management policy that will specify the procedures for establishing and communicating data breaches. In this context, the first of the following SLOs, as shown in Table 32, implements these principles and allows the customer to evaluate the suitability of the provider's policy.

The second SLO relates to the need to be prepared to demonstrate the setting up of the necessary measures to the competent supervisory authorities, upon request.

**Table 32: Accountability SLOs**

SLO	Description
Personal data breach policy	Describes the policy of the Shared Service Provider regarding data breach
Documentation	Refers to the list of the documents the provider makes available to demonstrate compliance to data protection requirements and obligations (e.g., procedures to respond to access request, designation of data protection officers, certifications, etc.)

- **GEOGRAPHICAL LOCATION OF SHARED SERVICE CUSTOMER DATA:**

Personal data processed in the shared service may be transferred, also by subcontracting, to third countries, whose legislation does not guarantee an adequate level of data protection.

To minimize these risks, the shared service customer should verify the provider guarantees lawfulness of cross-border data transfers. To this end, the shared service

customer will be made aware of the location of data processed in the cloud, as required also by the above-mentioned principles of openness and transparency.

In this context, the following SLOs, as shown in Table 33, represent the instruments based on which the shared service customer is allowed to control the location of its data.

**Table 33: Geographical Location of Shared Service Customer Data**

<b>SLO</b>	<b>Description</b>
Data geolocation list	Specifies the geographical location(s) where the shared service customer data may be stored and processed by the Shared Service Provider
Data geolocation selection	Specifies whether the shared service customer can choose a given geographical location for the storage of the shared service customer data

## Appendix C: Use Case Narratives

Use cases are useful for describing the intended sequence and interaction of components. The IT Security Continuous Monitoring Shared Services SECONOPS is fundamentally based on the Security Attributes and expressed through use cases. The definition for a use case is a description of system behavior, in terms of sequences of actions. A use case should yield an observable result of value to an actor. A use case contains all flows of events related to producing the "observable result of value," including alternate and exception flows.

More formally, a use case defines a set of use case instances or scenarios. An actor is someone or something outside the system that interacts with the system.<sup>24</sup> Other diagram elements represent components of the system that perform a function. Sequence diagrams show interactions between objects/actors as a series of events shown by a line with an arrow showing the direction of the message. A message with a dashed line shows a response to a message. A message internal to an object/actor is shown as a loop back.

This section describes some of the various high-level, security-relevant use case scenarios that IT Security Continuous Monitoring Shared Services may use. These use cases illustrate scenarios for:

- How data is collected
- How vulnerability data can be accessed/reviewed by a portal
- How vulnerability data is obtained from the National Vulnerability Database (NVD)
- How IT Security Continuous Monitoring Shared Services tracking and monitoring data is accessed
- How an organization may obtain IT Security Continuous Monitoring Shared Services
- How IT Security Continuous Monitoring Shared Services is backed up

Use case scenarios, suggested sequence diagrams, and suggested security strategies illustrate an example of a method and do not presuppose or mandate any particular solution or method. Due to the conceptual nature of use case scenarios, the use cases do not cover all aspects of a fully implemented and secure system. Implementation of the exact depicted scenario should not be considered sufficient to meet all stakeholder requirements for security and function. They are useful, however, to allow Stakeholders to think through security-relevant aspects of the design in subsequent lifecycle phases.

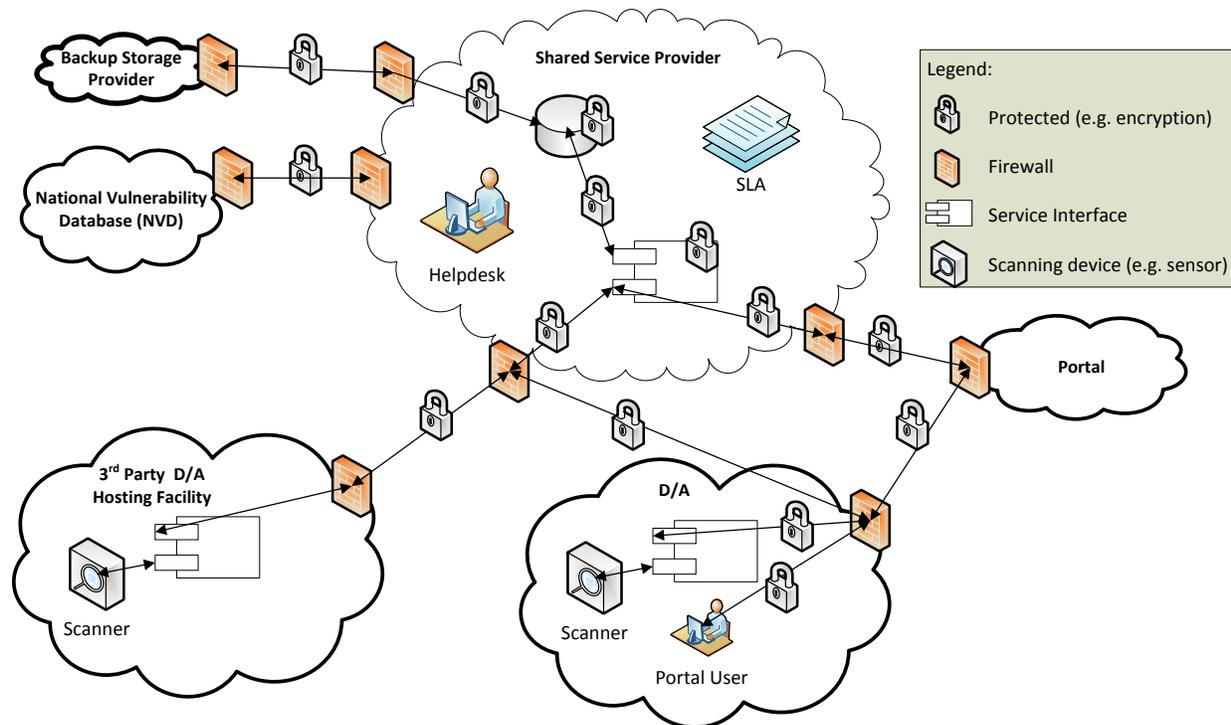
Some of the scenarios utilize Figure 14 below, which depicts one narrative, presenting IT Security Continuous Monitoring Shared Services hosted at a Shared Service Provider and a scanning device located at the Agency's site.

**NOTE:** The term "sensor" is used throughout the document as the typical scanning device. A sensor is just one option for vulnerability scanning; there are others (e.g., agents or scan engines).

---

<sup>24</sup> DoD Architecture Framework v 1.5

The diagram also takes into account the scanning of Agency items that may be outsourced or reside at other Agency locations. The term “portal” represents a generic portal that represents the IT Security Continuous Monitoring dashboard or other portals that may be needed to support the IT Security Continuous Monitoring Shared Services. For example, a non-IT Security Continuous Monitoring portal could provide access to system metrics or logs.



**Figure 14: IT Security Continuous Monitoring Shared Services Overview for Narrative Use Cases**

Figure 15 below shows the complexity of IT Security Continuous Monitoring Shared Services and Agency data. It is important to define what data is being referenced in this document, since data regarding Agency systems and Shared Service Infrastructure exists outside the scope of IT Security Continuous Monitoring Shared Services. There are layers of data and logs and the Agency’s infrastructure and security plans should address how to handle them securely.

IT Security Continuous Monitoring Shared Services only has data related to Agency enterprise IT assets and their vulnerabilities (e.g., hardware/software asset inventories, vulnerability scan report results). The key point is that IT Security Continuous Monitoring Shared Services does not store Agency sensitive mission-related data (e.g., Personally Identifiable Information (PII)) beyond the vulnerability information associated with the systems. Another point is that the Shared Service Provider will have data regarding its infrastructure not related to IT Security Continuous Monitoring Shared Services. The IT Security Continuous Monitoring Shared Services data specific to a Agency will be accessible by that Agency and no other Agency.

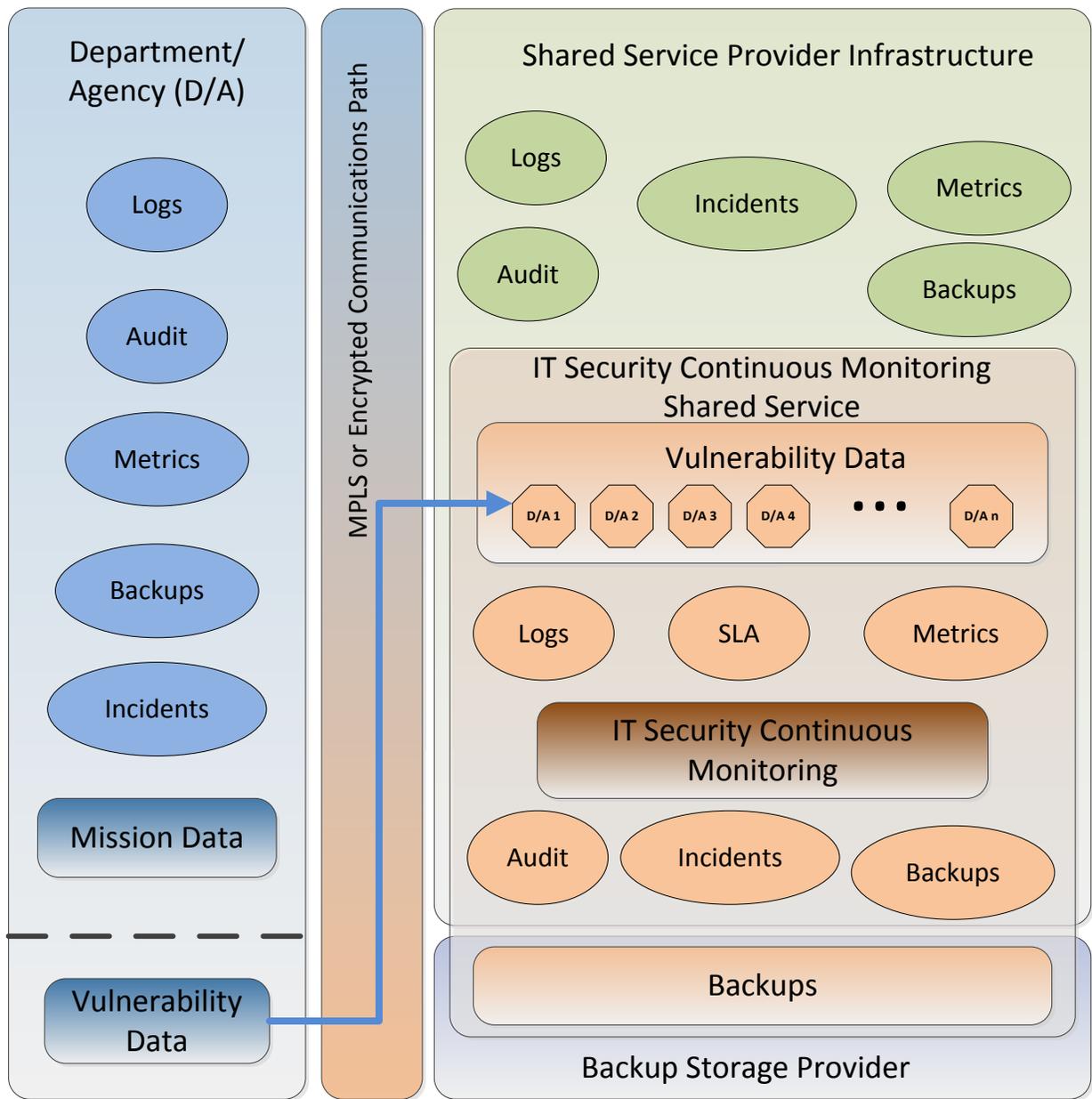


Figure 15: IT Security Continuous Monitoring Shared Services, Agency, and Shared Service Provider Data Locations

### C.1 Data Collection and Sensor Management

Data collection is a major component of the IT Security Continuous Monitoring Shared Services system. The IT Security Continuous Monitoring Shared Services needs to be able to obtain information about the Agency’s enterprise so that it can process the information and provide the Agencies the information they need via a portal. The information initially includes but is not limited to hardware, software, configuration, and vulnerability data for the Agency’s assets. The scenarios below address some notional ways that IT Security Continuous Monitoring Shared Services can obtain this data. Data Collection Scenario 1 shows IT Security Continuous

Monitoring Shared Services communicating directly with the Agency's sensors via a secure communication method. Data Collection Scenario 2 shows how IT Security Continuous Monitoring Shared Services scanning the Agency remotely in a manner not requiring any IT Security Continuous Monitoring Shared Services equipment at the Agency's site. Scenario 2 has several security and technical issues that may render it impractical in the near term, but may become an alternative in the future as available technologies and IT Security Continuous Monitoring Shared Services evolve. Data Collection Scenario 1 shows the simplest and most straight forward way based on commonly used technologies that are currently employed. One potential problem with Scenario 1 is that it may be impractical for the service to directly communicate with the sensors. This problem can be resolved with a sensor manager/aggregator, as shown in Sensor Management Scenario 1.

### **C.1.1 Data Collection Scenario 1**

The following model illustrates a possible sequence in which data is collected in a controlled and secure manner. The narrative sequence is as follows: the IT Security Continuous Monitoring Shared Services system in the shared service environment will send a request to the IT Security Continuous Monitoring Shared Services monitoring/data collection sensor residing at the Agency's location. The sensor, which has been collecting data for up to 72 hours, sends the collected data in an encrypted and digitally-signed format to the IT Security Continuous Monitoring Shared Services system in the shared service environment, as shown in Figure 15. Figure 16 shows the specific steps of the flow using a sequence diagram.

**NOTE:** The monitoring/data collection sensor could be owned by IT Security Continuous Monitoring Shared Services or by the Agency.

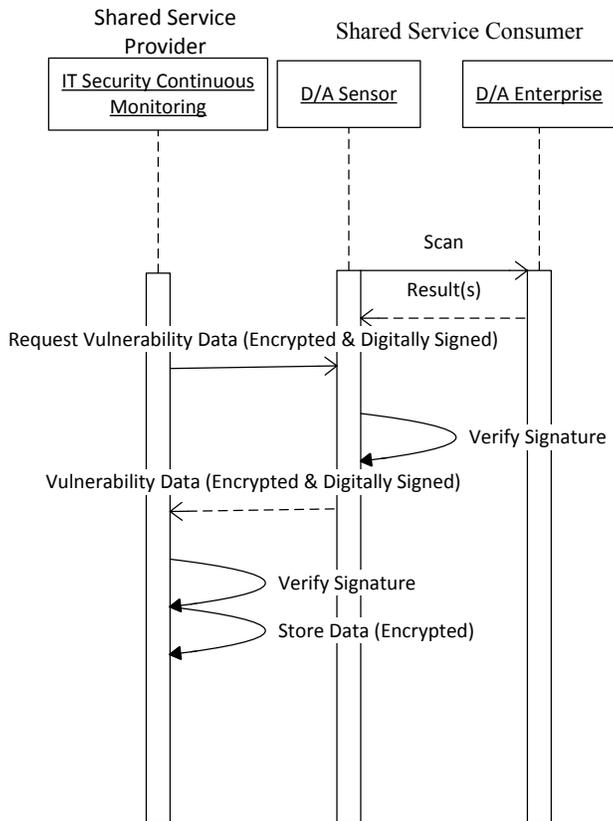


Figure 16: Data Collection Scenario 1 Sequence Diagram

### C.1.2 Data Collection Scenario 2

This scenario illustrates another potential IT Security Continuous Monitoring Shared Services implementation that enforces the security objectives of this SECONOPS. The narrative sequence is as follows: the IT Security Continuous Monitoring Shared Services system in the shared service environment will scan the Agency’s systems remotely via a to-be-determined connectivity communications link. The scans will be distributed over time to limit the bandwidth impact on communication path(s) between IT Security Continuous Monitoring Shared Services and the Agency. Scans will occur at least every 72 hours. The data will be encrypted as it traverses the communication link. The sequence diagram for this scenario is shown in Figure 17 below.<sup>25</sup>

<sup>25</sup> While this alternative may be a possibility in the future, currently most of the Agencies firewall policies do not permit scanning from outside of their Enterprise. Secondly, most sensor devices would not support directly being queried with an encrypted message and signing any response. This solution also presents concerns with load balancing and bandwidth queried with an encrypted message and signing any response.

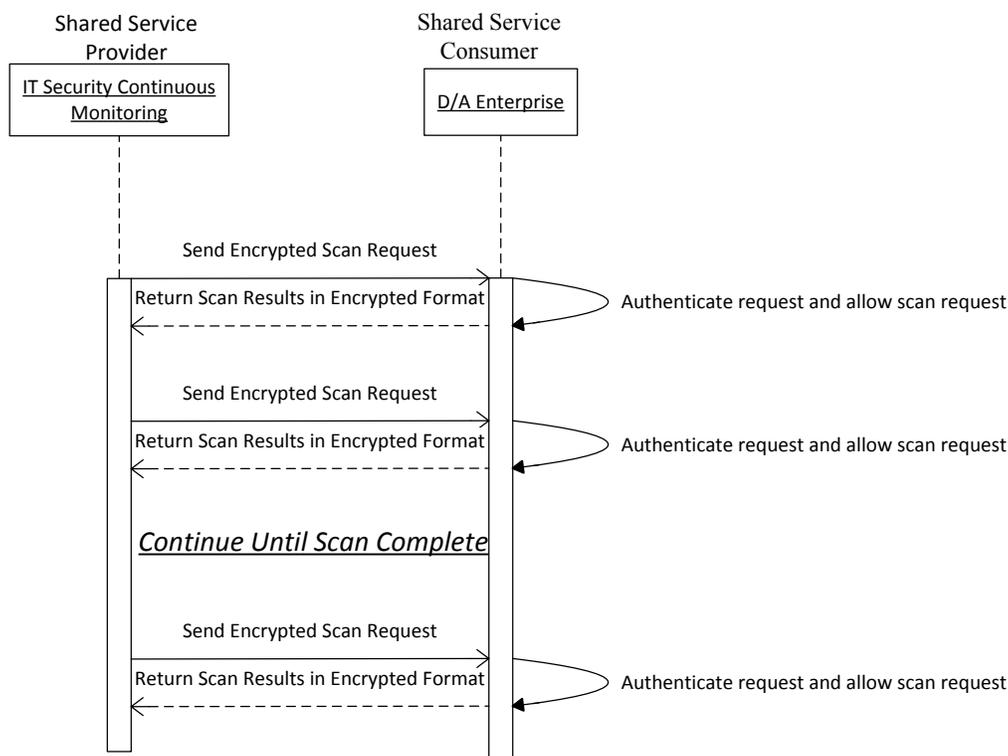


Figure 17: Data Collection Scenario 2 Sequence Diagram

### C.1.3 Sensor Management Scenario 1

The communication and aggregation of sensor data back to IT Security Continuous Monitoring Shared Services should account for the following items:

- How will the sensor data be collected?
- How will it be aggregated?
- How will the sensor data be transferred to IT Security Continuous Monitoring Shared Services?

This scenario addresses the location of sensors, how the sensor data is collected or aggregated, and includes potential IT Security Continuous Monitoring Shared Services components internal to the Agency's infrastructure. Much of how this might work will be dependent on the capabilities of the sensors and what the Agency will allow through their internal firewalls.

Sensors will most likely only be allowed to scan those device/servers located on a specific subnet or router enclave, as shown in Figure 18. This may necessitate a Sensor Manager to collect/aggregate the sensor data. Only the Sensor Manager would be able to communicate through the internal firewall to the Demilitarized Zone (DMZ). Figure 19 shows the Sensor Manager communicating with a IT Security Continuous Monitoring Shared Services Agent, which in turn communicates with the shared service. Figure 19 shows a notional sequence of events.

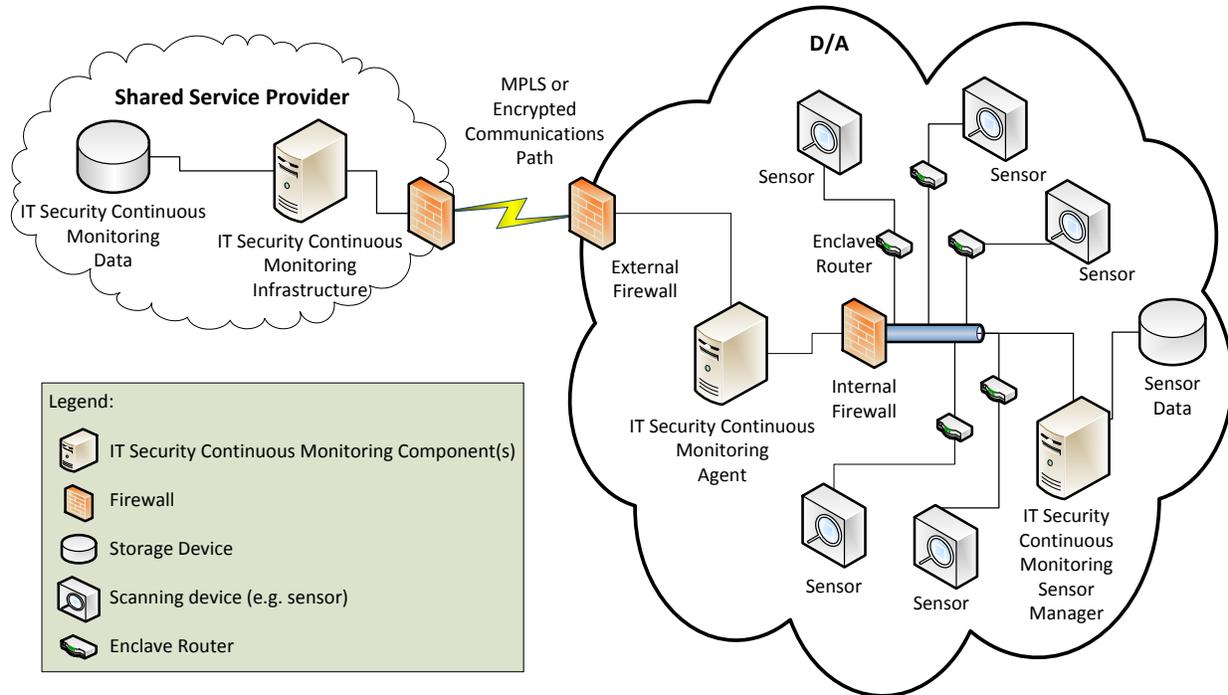


Figure 18: Sensor Management Scenario 1

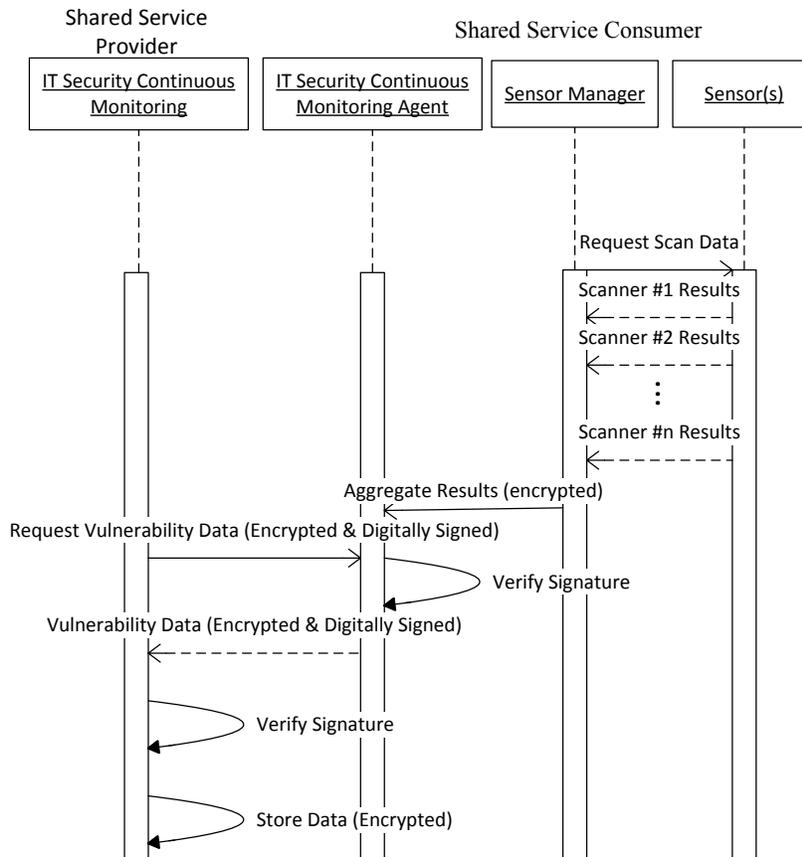


Figure 19: Sensor Management Scenario 1 Sequence Diagram

## C.2 Portal Scenarios

The end user will access IT Security Continuous Monitoring Shared Services data via one or more portals, including the IT Security Continuous Monitoring dashboard. Portal Scenario 1 shows how a user can access the IT Security Continuous Monitoring dashboard, including authentication and encryption of traffic between the user and the portal and between the portal and the service which hosts the data. It is likely the portal will be accessed via a browser and the Browser Considerations Scenario provides information that should be considered if that is the solution.

The scenarios for High Level Tracking and Monitoring of IT Security Continuous Monitoring Shared Services and O&M and Low Level Tracking and Monitoring of IT Security Continuous Monitoring Shared Services show how and who can access data related to these IT Security Continuous Monitoring Shared Services specific data. Similarly, the Access to Audit Logs Scenarios show how and who can access that IT Security Continuous Monitoring Shared Services audit data.

### C.2.1 Portal Scenario 1

The questions of how a user can access data securely and how that access is controlled in a shared environment are fundamental security concerns of a shared service. In this scenario, the collected data is posted on the Agency’s portal residing in the shared environment and is only

available to those individuals authorized by the Agency. Communication between the authorized user and the portal will be encrypted. In addition, multifactor authentication may be specified, such as certificate-based authentication (e.g., Personal Identity Verification (PIV) card). The individual portal views will not be available to anyone outside the Agency’s purview. The sequence diagram for this scenario is shown in Figure 20 below.

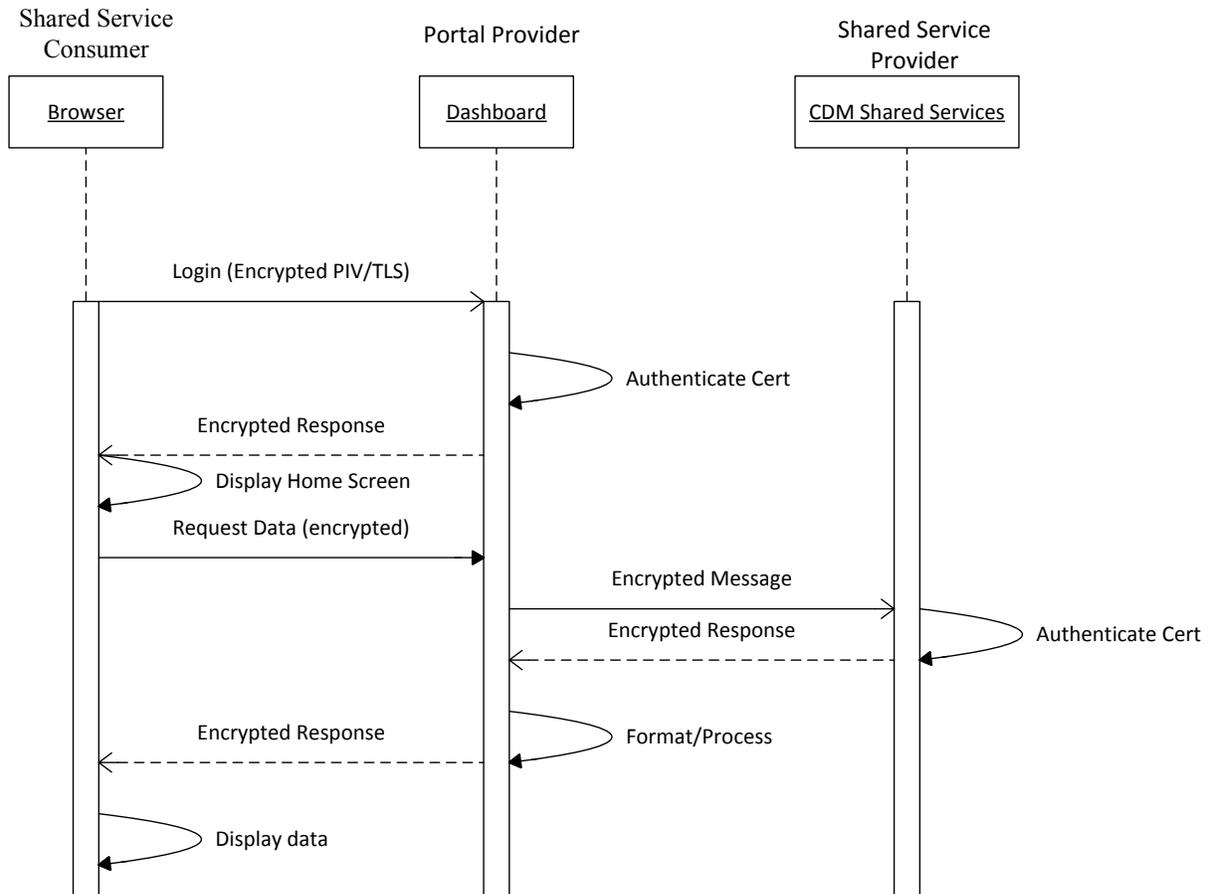


Figure 20: Portal Scenario 1 Sequence Diagram

### C.2.2 Browser Considerations Scenario

This scenario takes into account that the user community IT infrastructure will be heterogeneous, and that IT Security Continuous Monitoring Shared Services will specify minimum, acceptable software standards for access to the system. This specific use case discusses browser considerations as the most likely method for user connectivity to the IT Security Continuous Monitoring Shared Services portal, but there may be other software requirements as well. The use case narrative is as follows: the user will connect to the IT Security Continuous Monitoring Shared Services portal with a browser (e.g., Internet Explorer, Firefox, and Chrome). Users authorized by Agency should have a Government- owned computer that has current patches for the operating system, browser, and applications.

The use of mobile code<sup>26</sup> should be carefully considered since it can be used as a vector to exploit vulnerabilities on a personal computer. Any mobile code that can access resources beyond the browser's sandbox should be avoided. The computer should also have current virus protection. The browser will support the minimum and most current encryption level supported by IT Security Continuous Monitoring Shared Services for Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol transactions. The authentication method will utilize multifactor authentication, a Virtual Private Network (VPN) connection, or combination of both. The computer utilized will only access the portal from a protected Government network. Policies considering Bring Your Own Device (BYOD) and/or connectivity from other non-Government networks/devices should be addressed and fully documented and accepted by senior management. Device connectivity to systems or data should be within acceptable parameters deemed appropriate by the mission stakeholders. This can be enforced through policy or technically enforced.

### **C.2.3 Update Portal Data Scenario 1**

IT Security Continuous Monitoring Shared Services sensors automatically collect data regarding all enterprise assets and associated vulnerabilities. The IT Security Continuous Monitoring Shared Services portal also allows Agency designated individuals edit access to some of the Agency's supplementary data in the portal. Some examples are the ability to add or edit the Agency Point of Contact (POC) for assets or a POA&M regarding a vulnerability or additional information about an asset. Communication between each designee and the portal will be encrypted. Each Agency will only have access to its own data. The sequence diagram for this scenario is shown in Figure 21.

---

<sup>26</sup> Mobile code is software transferred between systems (e.g., transferred across a network, and executed on a local system with or without explicit installation by the recipient). The mobile code may remain resident on the local system

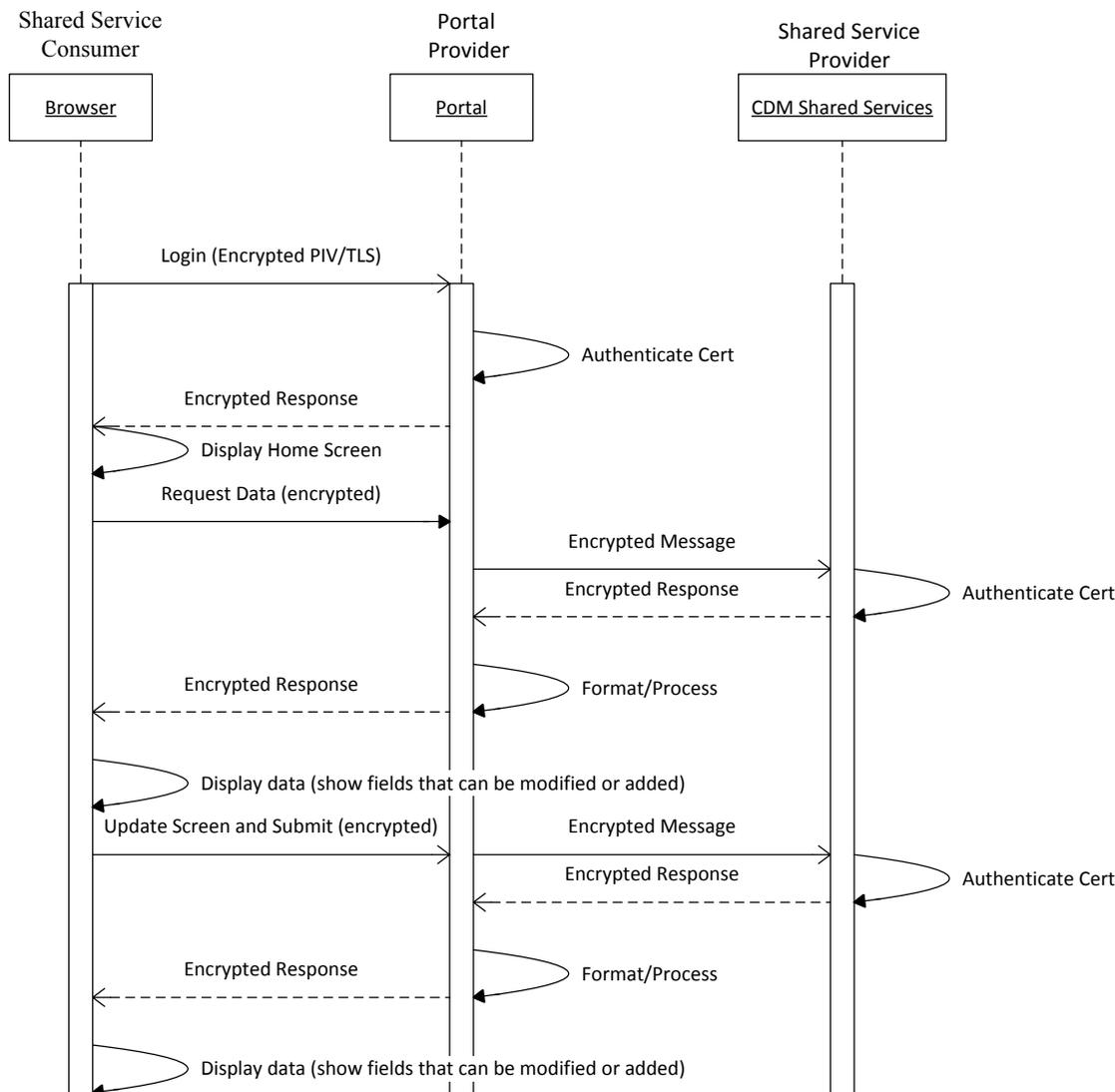


Figure 21: Update Portal Scenario 1

### C.2.4 High Level Tracking and Monitoring of IT Security Continuous Monitoring Shared Services Scenario 1

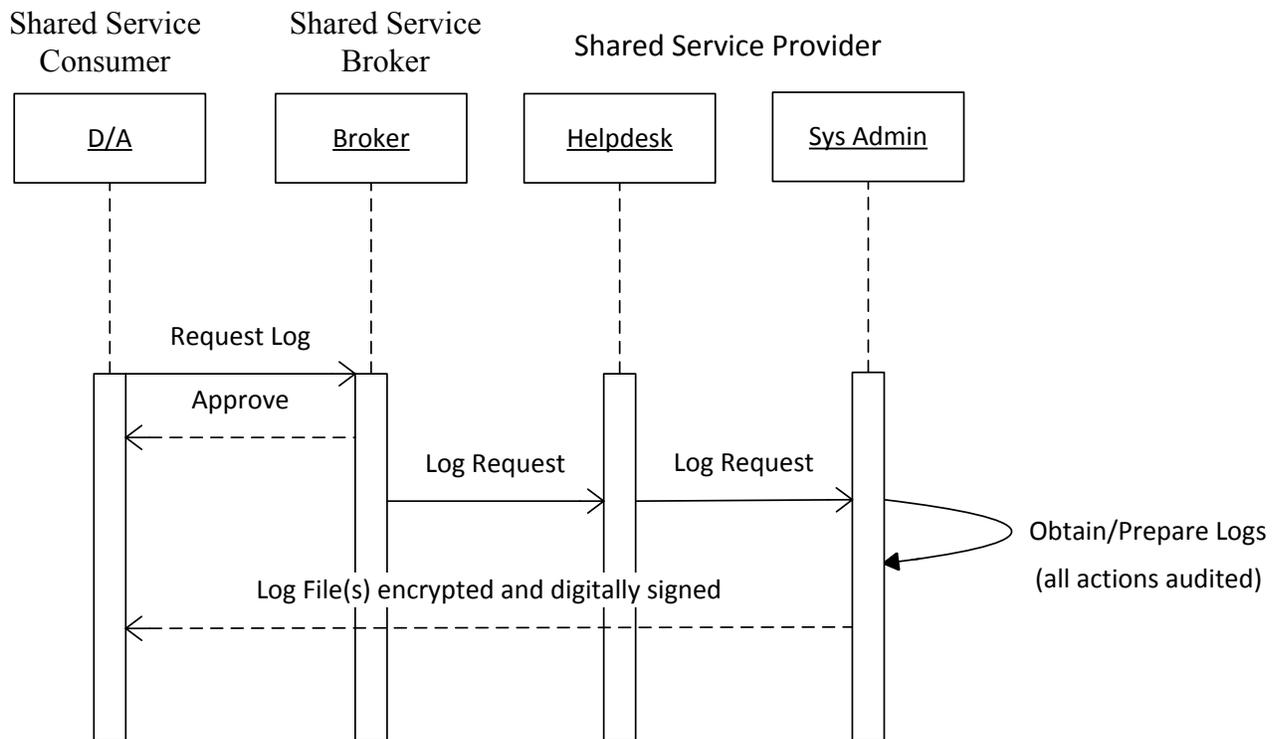
Certain users identified by DHS and/or its acquisitions service provider and Agencies will have access to Shared Service Provider IT Security Continuous Monitoring Shared Services metrics and/or be able to track and monitor certain aspects of IT Security Continuous Monitoring Shared Services. The metrics, tracking and monitoring information would be available via a portal. Communication between each designee and the portal will be encrypted. The individual report within the portal will not be available to anyone outside the specific Agency’s purview. Access to this information will be tightly controlled and monitored using the security controls outlined in the System Security Plan. The sequence diagram for this scenario is almost identical to that shown in Figure 20. The only difference is that the user has been authorized to see metrics data and will have that as an option to access.

### C.2.5 O&M and Low Level Tracking and Monitoring of IT Security Continuous Monitoring Shared Services Scenario 1

The Shared Service Provider will perform routine Operation and Maintenance (O&M) activities including tracking and monitoring IT Security Continuous Monitoring Shared Services for proper operations and security posture. All activities required by the SLA should be documented in the appropriate manual (e.g., System Administrators Manual, Routine Maintenance Manual, and Trusted Facilities Manual) as processes and procedures readily available to all appropriate personnel at the Shared Service Provider. All activities performed by any personnel will be done through an account assigned to a single individual. Group/shared passwords should not be used. The sequence diagram for this scenario is almost identical to that shown in Figure 20. The only difference is that the user has been authorized to view metrics data and will have that as an option to access.

### C.2.6 Access to Audit Logs Scenario 1

Shared Service Providers will obtain and provide audit logs to support an incident or other reporting requirements. Depending on their size, logs will be sent by encrypted and digitally signed e-mail or by another electronic or physical means that includes the appropriate FIPS level encryption. The sequence diagram for this scenario is shown in Figure 22.

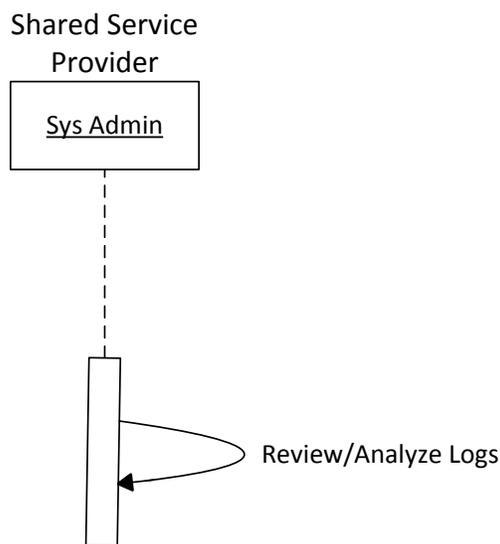


Note: All written communication is encrypted and digitally signed. If log file(s) are too large to be sent by email they will be sent by other means but will still be encrypted and digitally signed.

Figure 22: Access to Audit Logs Scenario 1 Sequence Diagram

### C.2.7 Access to Audit Logs Scenario 2

Shared Service Provider personnel assigned and approved to work on IT Security Continuous Monitoring Shared Services will have read-only access to all IT Security Continuous Monitoring Shared Services audit logs required to accomplish their duties. However, all access to the audit logs will be through individual user accounts with audit events. The sequence diagram for this scenario is shown in Figure 23.



Note: Logs are only accessed in accordance with documented process and procedures. All log access is by individual user account and is audited.

Figure 23: Access to Audit Logs Scenario 2 Sequence Diagram

## C.3 Order and Obtain IT Security Continuous Monitoring Shared Services Scenarios

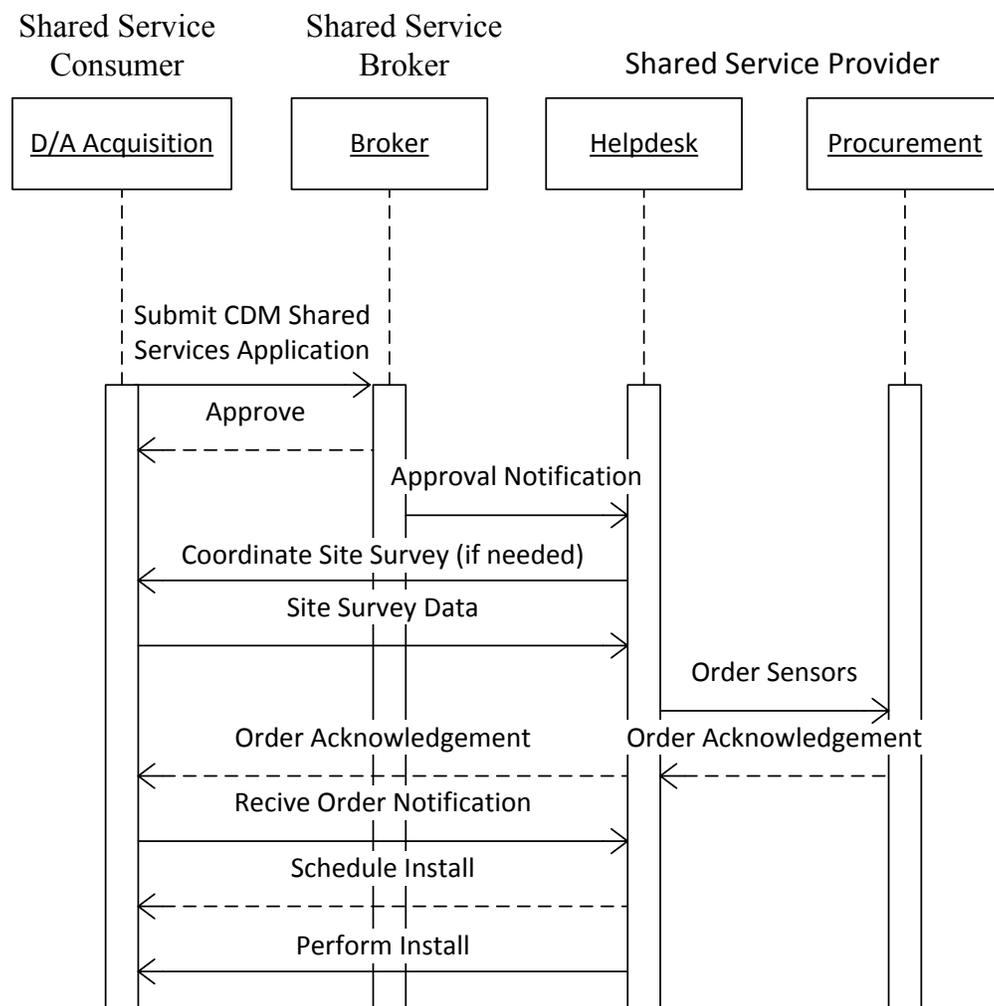
The following two scenarios show how an Agency can order and obtain IT Security Continuous Monitoring Shared Services. The primary difference between the two scenarios is who provides the sensors. The Shared Service Provider can provide the sensors, or they can be provided by the Agency, if they meet the requirements/specifications of IT Security Continuous Monitoring Shared Services.

### C.3.1 Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 1

The steps to order IT Security Continuous Monitoring Shared Services where the Shared Service Provider provides the sensors are shown below and in Figure 24.

1. Submit the appropriate forms and artifacts needed to obtain IT Security Continuous Monitoring Shared Services (e.g., IT Security Continuous Monitoring Shared Services Blanket Purchase Agreements)

- a. Include information regarding any outsourced third party site where Agency applications or services are hosted
2. After an Agency's request has been approved, the IT Security Continuous Monitoring Shared Services Help Desk contacts the Agency to determine if a site survey is needed. If needed, the IT Security Continuous Monitoring Shared Services Help Desk will coordinate and schedule the visit(s) with the Agency
3. Once all required information has been obtained, the IT Security Continuous Monitoring Shared Services components are ordered and shipped to the Agency site(s)
4. After the components(s) arrive, the Agency contacts the IT Security Continuous Monitoring Shared Services Help Desk to have the components(s) installed and configured
5. The Shared Service Provider or a designated third party will install and configure IT Security Continuous Monitoring Shared Services mechanism(s) at Agency site(s) including any third party outsources sites



Note: All written communication is via encrypted and digitally signed email.

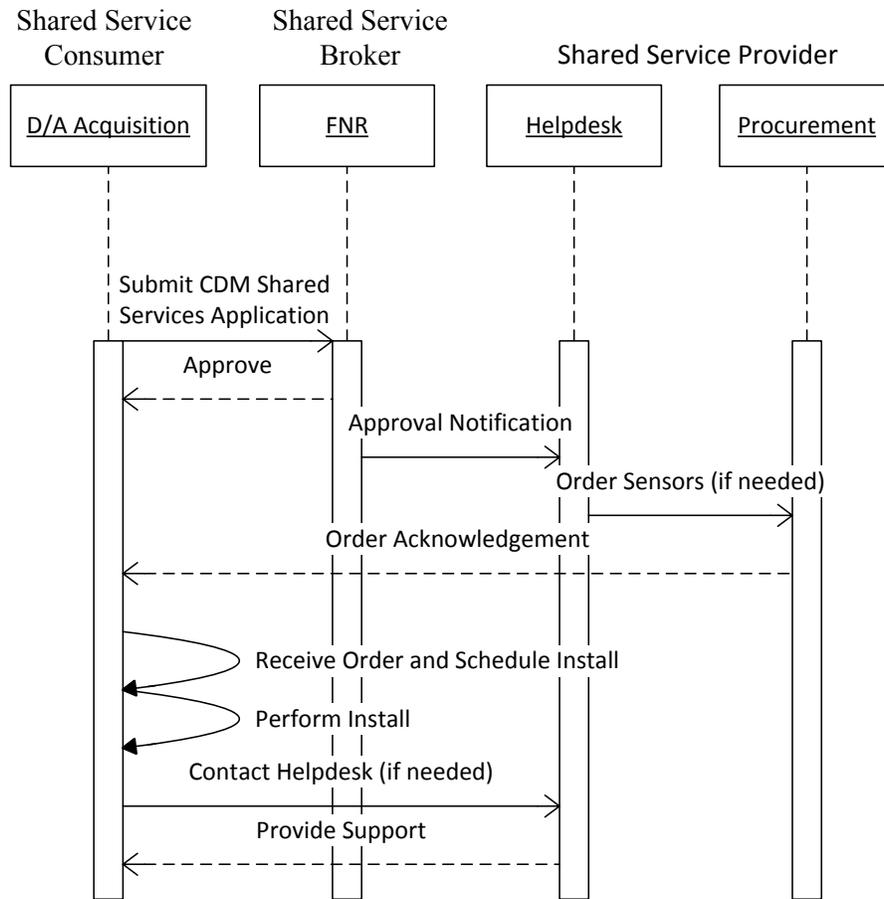
**Figure 24: Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 1 Sequence Diagram**

### C.3.2 Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 2

The steps to order IT Security Continuous Monitoring Shared Services where the Agency owns sensors are shown below and in Figure 25.

1. Submit the appropriate forms and artifacts needed to obtain IT Security Continuous Monitoring Shared Services (e.g., IT Security Continuous Monitoring Shared Services Blanket Purchase Agreements)
  - a. Include information regarding any outsourced third party site where Agency applications or services are hosted
2. After an Agency's request has been approved, the Agency, or its designate, installs and configures its sensors at the Agency site(s) including any third party outsourced sites

- a. Note the Agency is responsible for adding any additional sensors. It can contact the IT Security Continuous Monitoring Shared Services Help Desk for assistance if needed when installing or configuring their sensors



Note: All written communication is via encrypted and digitally signed email.

**Figure 25: Order and Obtain IT Security Continuous Monitoring Shared Services Scenario 2 Sequence Diagram**

### C.4 IT Security Continuous Monitoring Shared Services Backup Scenario 1

The Shared Service Provider will perform routine backups of all IT Security Continuous Monitoring Shared Services systems on a regular basis. The backups will be protected at all times and readily accessible to support restoration and Continuity of Operations (COOP). Two backups will be made; one stored on-site and one stored at an approved off-site storage facility. IT Security Continuous Monitoring Shared Services will use NIST backup guidelines,<sup>27</sup> taking into account the FIPS 199 Availability Impact Level of HHM as an additional guideline. The sequence diagram for this scenario is shown in Figure 26.

<sup>27</sup> NIST SP 800-123, “Guide to General Server Security”

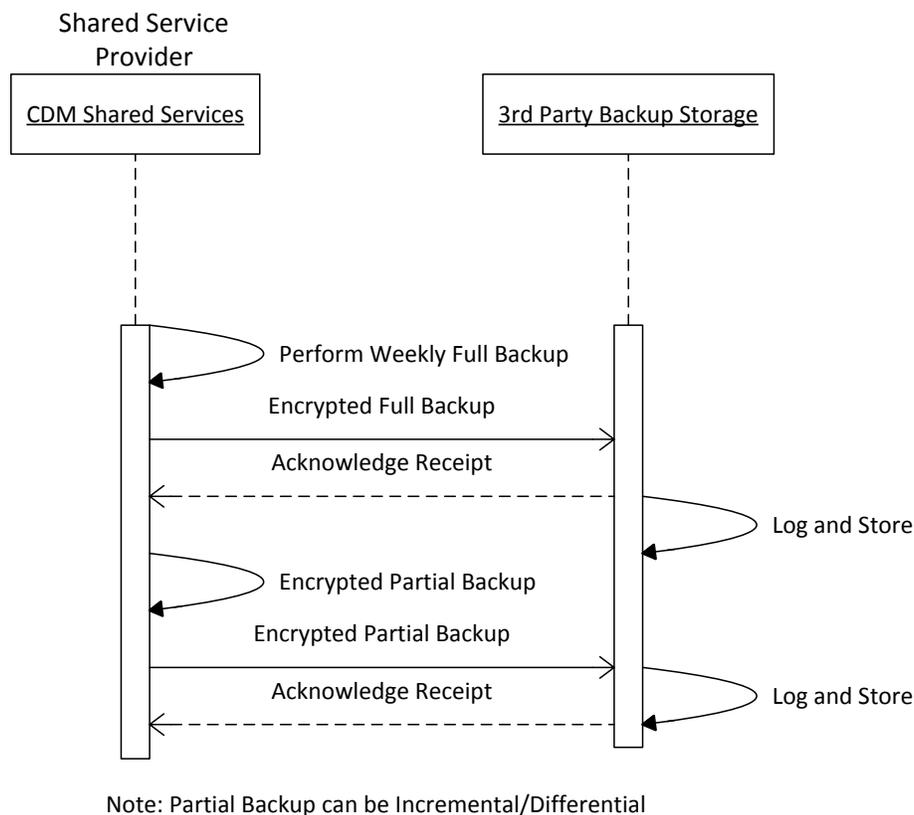


Figure 26: IT Security Continuous Monitoring Shared Services Backup Scenario 1 Sequence Diagram

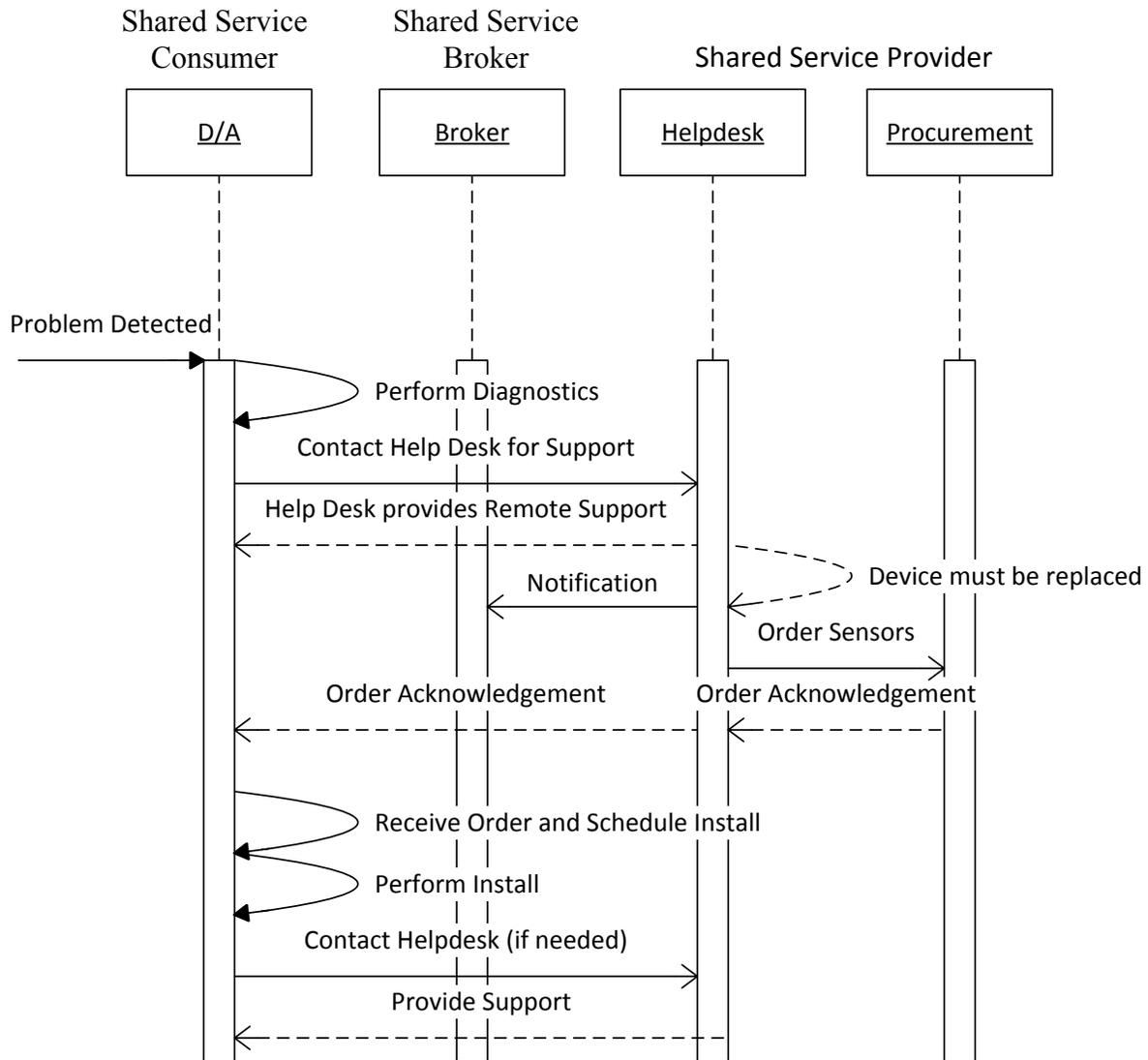
## C.5 Repair or Replace IT Security Continuous Monitoring Shared Services Component(s)

The following two scenarios show how IT Security Continuous Monitoring Shared Services components located at an Agency facility can be repaired or replaced. If the component is owned by the Agency, it is the responsibility of the Agency to repair the component. If the component is provided by the Shared Service Provider, then it is the responsibility of the Shared Service Provider to repair or replace the component. If the replacement is a simple swap, and both the Agency and Shared Service Provider agree, then the Agency may perform the swap.

### C.5.1 Repair or Replace IT Security Continuous Monitoring Shared Services Component(s) at Agency Site Scenario 1

If an issue is discovered with IT Security Continuous Monitoring Shared Services or one of the IT Security Continuous Monitoring Shared Services component(s) located at a Agency site, the Agency should contact the IT Security Continuous Monitoring Shared Services Help Desk for troubleshooting support. If the problem is isolated to a hardware failure at a Agency site, the IT Security Continuous Monitoring Shared Services Help Desk will obtain and ship a replacement to the Agency site. IT Security Continuous Monitoring Shared Services will ensure that Supply Chain Security controls are implemented when sourcing replacement components. When the component arrives at the Agency site, the Agency installs the new component and returns the old

one to the location specified by the IT Security Continuous Monitoring Shared Services Help Desk. The sequence diagram for this scenario is shown in Figure 27.



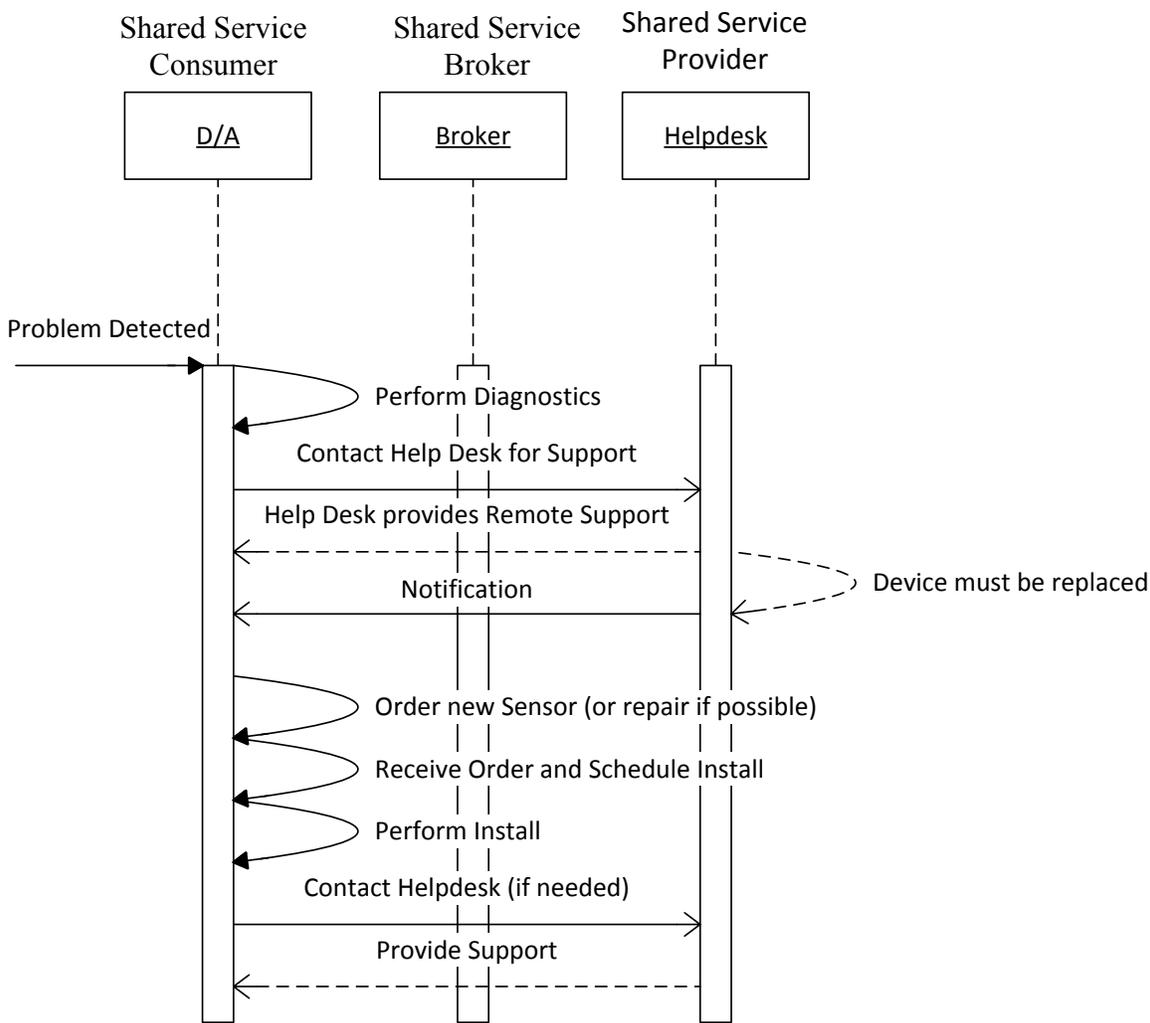
Note: All written communication is via encrypted and digitally signed email.

Figure 27: Repair or Replace IT Security Continuous Monitoring Shared Services Component(s) at Agency Site Scenarios 1 Sequence Diagram

### C.5.2 Repair or Replace IT Security Continuous Monitoring Shared Services Component(s) at Agency Site Scenario 2

If an issue is discovered with IT Security Continuous Monitoring Shared Services or one of the IT Security Continuous Monitoring Shared Services components located at an Agency site, the Agency should contact the IT Security Continuous Monitoring Shared Services Help Desk for support. If the problem is isolated to a hardware failure at an Agency site and owned by the Shared Service Provider, the IT Security Continuous Monitoring Shared Services Help Desk will obtain and ship a replacement to the Agency site as shown in Scenario 1. If the component is owned by the Agency, it is the Agency’s responsibility to repair or replace the component, as

shown in Figure 28. If the Agency would prefer to switch and use the component provided by the Shared Service Provider, then it would need to coordinate with the Shared Service Provider to make that change and then follow the procedures outlined in Scenario 1.



Note: All written communication is via encrypted and digitally signed email.

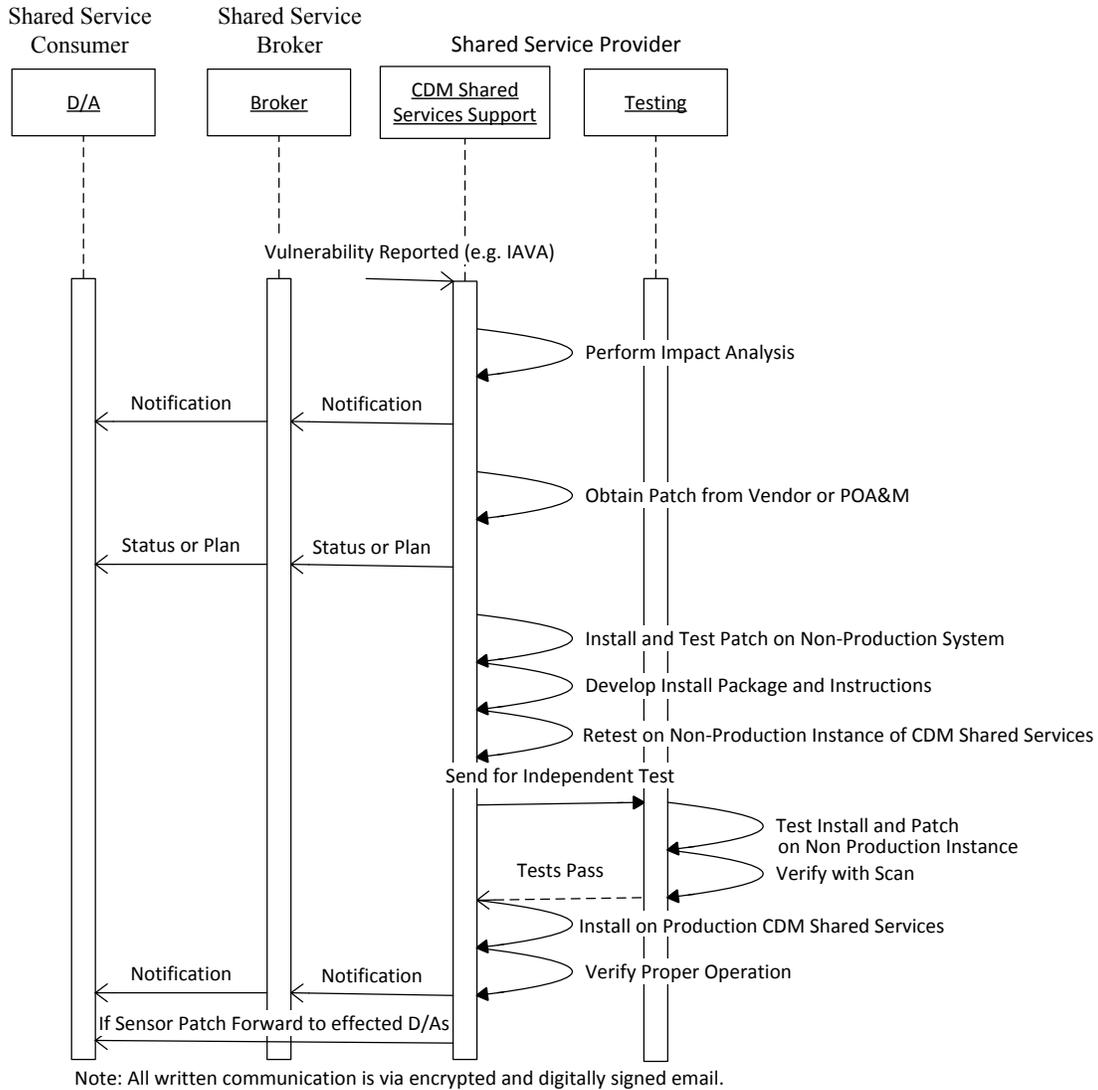
**Figure 28: Repair or Replace IT Security Continuous Monitoring Shared Services Component(s) at Agency Site Scenarios 2 Sequence Diagram**

### C.6 Patch IT Security Continuous Monitoring Shared Services Scenario 1

Figure 29 shows the major steps that occur when an Information Assurance Vulnerability Alert (IAVA) is released that may impact IT Security Continuous Monitoring Shared Services. This process includes determining any impact to sensors provided by IT Security Continuous Monitoring Shared Services. Once the IAVA notification is received, the Shared Service Provider performs an impact analysis within the time specified in the SLA (e.g., 24 hours). The Shared Service Provider then notifies the Agencies of the results of its analysis via a secure method (e.g., an encrypted and digitally-signed email).

If IT Security Continuous Monitoring Shared Services or the sensors are not impacted, then no further action is required. If IT Security Continuous Monitoring Shared Services is impacted, the Shared Service Provider obtains the patch from the vendor and then installs and tests it on a non-production instance of IT Security Continuous Monitoring Shared Services. If, for some reason, a patch is not available or the patch would interfere with IT Security Continuous Monitoring Shared Services normal operations, then a POA&M is developed. The POA&M will describe the intended approach, milestones, and timeline to resolve the vulnerability and what mitigation steps will be taken until the vulnerability can be patched. Once the support team has fully tested the patch, including the associated installation packages and instructions, it is sent for independent testing. This independent test and evaluation will be performed by an individual or group in a separate reporting chain not directly affiliated with the individual or team who performed the initial testing.

The SLA will specify if the Shared Service Provider can perform the test or whether a third party will perform the test. The SLA should also specify if the final test will be witnessed by another party (e.g., FNR). Since vulnerabilities need to be closed as quickly as possible, the level of testing and the number of organizations that should coordinate the test should be kept as small as is reasonable, while still maintaining strict CM control. Not shown in Figure 29 is any required Configuration Control Board (CCB) approvals and notification to Agencies prior to installing the patch on the production system.



**Figure 29: Patch IT Security Continuous Monitoring Shared Services Scenario 1**

## Appendix D: IT Security Continuous Monitoring Shared Services Operational Security Principles

IT Security Continuous Monitoring Shared Services security will be a shared responsibility for all roles, stakeholders, and users. It is intended that IT Security Continuous Monitoring Shared Services will implement sufficient security controls to ensure it conforms to the threat and compliance mandates. These controls follow the families of controls listed in NIST 800-53 Revision 4. The following section provides a general overview of the security objectives and controls. Specific applications of controls and requirements will be in subsequent SSPs and other design documents.

At a minimum, any shared system/service should be evaluated to ensure it meets the security requirements in the following categories for the specific system:

- Confidentiality
- Integrity
- Availability
- Authentication and Authorization
- Identity Management
- Security Monitoring
- Incident Response
- Policy Enforcement
- SLA
- Quality of Service (QoS)

Additionally, the security of the virtualized system should follow security guidelines such as outlined in the NIST SP 800-125 A: “DRAFT Security Recommendations for Hypervisor Deployment” and the book “Virtualization Security: Protecting Virtualized Environments” by David Shackelford, Sybex publishers, ISBN-10: 1118288122.

A key aspect of the security framework for IT Security Continuous Monitoring Shared Services was to establish the attributes necessary for consideration as part of a HHM baseline for a shared service. These attributes were developed using a top-down approach derived from the SABSA approach. Appendix A contains the SABSA Attribute Chart and attribute definitions.

### D.1 Protection of Data

The SLA for the IT Security Continuous Monitoring Shared Services Provider will stipulate how data is protected at rest and in transit IAW any applicable Government laws, regulations, mandates and directives. IT Security Continuous Monitoring Shared Services data is very sensitive since it contains vulnerability data that can be exploited if disclosed. The data for each Agency will be separated through the use of access controls that will provide logical separation of each Agency’s data. This is especially important if the Shared Service Provider is also hosting commercial customers using the shared infrastructure. Data from each Agency will also be separated so that it is not disclosed to a person who is not appropriately authorized. Contract

clauses will further define how separation and access to the data should be implemented. In addition, the following should be addressed in the SLA:

- Non-government tenants must be physically separated from government tenants.
- If VMs are utilized, they will be tracked and monitored.
- The data for each Agency will be separated through the use of access controls that will provide logical separation of each Agency's data.
- Similarly, for a network configuration, protections mechanisms, policies, and procedures will be clearly defined and articulated. This will include both physical and logical (i.e., software defined) implementations of the networks.
  - The protection of the vulnerability data is critical, and therefore private, dedicated encrypted communication paths (i.e., Multi-Protocol Label Switching) should be considered.
- Define how, when, and where data is backed up, and specifically how the backed up data is protected.

## **D.2 Location of Data**

In a shared environment the location of data, services, and communications paths are not always known to the service user. The Shared Service Provider could utilize resources to provide the service potentially from any part of the world. The laws, regulation, and threats vary widely in different countries. Therefore the SLA with IT Security Continuous Monitoring Shared Services should stipulate that the allowed physical/geographical locations for services, communication paths, and data including the location of any copies or backups will be Continental United States (CONUS) only.

Communications paths between IT Security Continuous Monitoring Shared Services and Agency sites may need to cross country boundaries (e.g., US Embassies). In those cases, the only communication data allowed to cross country boundaries will be the data for that specific Agency site, located in a foreign country; no other traffic will go outside of CONUS.

## **D.3 Communication Link Compromise**

Should a dedicated communication link be compromised, the Agency will have the ability to close the link. If the Agency cannot close the link, a mechanism will be in place to notify the Shared Service Provider and the provider will secure the port until the compromise is mitigated. Approved policies and procedures will be established to minimize erroneous shut down of the dedicated link.

## **D.4 Visibility of Data by Shared Service Provider**

The SLA with the Shared Service Provider will stipulate who can view the data, what data they can view, and under what circumstances. Additional requirements for US Citizen-only access to physical and logical components should be clearly stated if this is a requirement. If there is a requirement for security clearance, this should also be documented and agreed upon. Lastly, the SLA should document how access is controlled, monitored, and audited.

## **D.5 Visibility of Data by Agency**

The following will be considered when developing the SLA:

- Define the metrics regarding the service and link to IT Security Continuous Monitoring Shared Services the Shared Service Provider will provide
- Define when, how, and to whom notification of a confirmed or suspected data breach will be communicated
- Define what level of control Agencies will have over their data

## **D.6 Key Management**

A key management plan will be developed and approved before encryption keys are deployed. IT Security Continuous Monitoring Shared Services will use NIST SP 800-57, “Recommendation for Key Management,” July 2012, as a guideline. The master key to IT Security Continuous Monitoring Shared Services encryption will be stored in an approved and secure manner.

## **D.7 Termination or Transfer of Service**

If an event transpires rendering the Shared Service Provider incapable, regardless of the specific event, SLA’s shall define a clear plan and process to assure that all data including backups are gracefully transferred. No remnants of the data will be allowed to remain on or in the SSP environment, physically or logically. This could include physically removing all media, including hard drives from the Shared Service Provider. Obtaining the hard drives may be difficult since the storage media could be a Storage Area Network (SAN) or other shared storage media. This would mean some other mechanism for scrubbing data from the storage data may be needed. The mechanism for scrubbing will be in accordance with the HHM baseline and applicable NIST controls. This is particularly important if the shared service is provided by a commercial entity.

## **D.8 Shared Service Provider Notice of Termination**

In a shared service environment the consumers are dependent on the Shared Service Provider providing the service. The contract with the Shared Service Provider will stipulate the following:

- The Shared Service Provider shall give a minimum number of months (e.g., 12 months) notice before terminating the service IAW contract clauses. This will allow transition time to move to another Shared Service Provider, including overlap of 30 calendar days to ensure there is continuity of service and time for Agencies to test and transition. Should an unforeseen event/disaster occur, the SSP will work with the Acquisitions Service provider and SSP contract owner to plan for any transition or termination of service.
- Ensure there is an approved plan in place to transfer the service

## **D.9 Shared Service Provider Viability**

For a variety of reasons, the Shared Service Provider could go out of business unexpectedly. To mitigate the impact of such an occurrence, the Shared Service Provider will follow appropriate NIST guidelines. FNR manages the development/implementation of a transition plan to migrate IT Security Continuous Monitoring Shared Services to a new Shared Service Provider should the need arise.

To minimize such an incidence, an acquisitions service provider will carefully monitor the financial health of the Shared Service Provider and if the Shared Service Provider is a private concern, an acquisitions service provider will monitor the financial stability of the private concern's principle owners. If it is determined that the Shared Service Provider is undergoing financial difficulties, DHS Acquisitions Service provider, in coordination with DHS, shall, at its discretion, relocate IT Security Continuous Monitoring Shared Services to another Shared Service Provider and will notify Agencies IAW contract clauses and SLA's. If IT Security Continuous Monitoring Shared Services data is moved, data remnant removal will occur as outlined in Section D.7, Termination or Transfer of Service, above.

## **D.10 Shared Service Provider Survivability**

In case the Shared Service Provider suffers a natural or manmade disaster at its primary site, the Shared Service Provider will follow appropriate NIST guidelines. Guidelines for primary site failure and consequences for failing to meet the agreed notification time are addressed in the high baseline and relevant contract.

## **D.11 Protection of Service/System Management Function**

The management functions to administer and maintain the service/system in a shared environment will be protected at a higher level than how a IT Security Continuous Monitoring Shared Services general user accesses. While the IT Security Continuous Monitoring Shared Services data is highly sensitive and will be protected at a high level, the management functions could be used to compromise the whole service. Ideally, the management function requires on-site physical access to either a management console or via a separate physical or virtual network. It is particularly important to have additional security controls to limit the risk of unauthorized individuals accessing the IT Security Continuous Monitoring Shared Services management function from the internet. For example, multifactor authentication (with possibly more than just 2 factors), restricting incoming Internet Protocol (IP) addresses, automatic locking of accounts after several failed access attempts will be considered and outlined in the System Security Plan. Some solutions will require balancing security controls vs availability.

## **D.12 Help Desk**

When issues occur, specific problem response, resolution times, and escalation times will be defined in SLA's and documented in the System Security Plan. The SLA with the Shared Service Provider will define the thresholds for the aforementioned items. In addition, the following will be covered:

- Define who a portal user should contact if they experience a problem accessing the portal and/or logging-in

### **D.13 Availability**

IT Security Continuous Monitoring Shared Services will support the availability requirements of the Agencies IAW their regulatory requirements for incident response.

### **D.14 Hardening**

All Shared Service Provider servers, networking devices/appliances, and any equipment where IT Security Continuous Monitoring Shared Services is stored, processed, or transmitted through will be hardened according to NIST Hardening Guides, and/or other applicable hardening guides.

### **D.15 Sensor Security Considerations**

Some Agencies currently have their own sensors they may want to continue to use. IT Security Continuous Monitoring Shared Services intends to support all sensors that meet the minimum security, interface, and functionality requirements of IT Security Continuous Monitoring and are on the BPA approved list (i.e., all sensors will support Security Content Automation Protocol (SCAP)).

All sensors should be obtained using the appropriate supply chain controls to ensure the sensor meets all specifications and come from an authorized approved source. Resellers will provide evidence of the material chain of custody and/or certificates of origin. A process should be in place to assure only genuine Original Equipment Manufacturer products are acquired. NIST guidance will be utilized.

### **D.16 Common Deployment Modes**

Computer security best/proven practices will be employed for all common deployment systems. This includes, but not limited to, industry established hardening guides, NIST security guidelines, and other proven practices. Security will not be limited to hardware and software but will also include technical, operational, and managerial policies and procedures.

### **D.17 Vulnerability Data**

As discussed in Section D.1, protection of IT Security Continuous Monitoring Shared Services data is extremely important. Data will be controlled so only those who are appropriately authorized can access the data. The data also should support the Federal Information Security Management Act (FISMA) reporting requirements but may be limited based on the automation level. Agencies will provide consistent data for a particular reporting date. To support this following should be considered:

- Time stamps on vulnerability data
- Mechanisms to obtain a snapshot of the security posture at a particular point in time
- Ability to obtain an extract and/or archive of the data for reporting purposes

### **D.18 Incident Response**

The Shared Service Provider will follow the NIST Incident Response Plan guidelines as defined in NIST's "Computer Security Incident Handling Guide," SP 800-61, Revision 2, August 2012. The Incident Response Plan will clearly identify breach notification procedures to include

Agencies. Existing incident response plans will be reviewed, and if they align with NIST's "Computer Security Incident Handling Guide," they can be incorporated with the IT Security Continuous Monitoring Shared Services Incident Response Plan. Incorporation will be on a case-by-case basis.

In general, the steps for an incident involving IT Security Continuous Monitoring Shared Services will adhere to the following:

- Notify US-CERT when a Shared Service Provider reports an incident
- Work with the Shared Service Provider s to resolve incidents by providing coordination with US-CERT
- Notify Shared Service Providers if the Agency becomes aware of an incident that a Shared Service Provider has not yet reported
- Notify the FEDRAMP Information Systems Security Officer (ISSO), FNR and affected Agencies if a Shared Service Provider has reported an incident

To ensure effective communication and awareness during incident response, IT Security Continuous Monitoring Shared Services Incident Response will be coordinated among Agencies and the Service Provider in accordance with DHS and US CERT guidelines.

## **D.19 IT Security Continuous Monitoring Shared Services Monitoring**

IT Security Continuous Monitoring Shared Services will be a key component in providing assurance to Agencies. As such, there should be a mechanism to ensure IT Security Continuous Monitoring Shared Services continues to meet its own security posture and mission. While IT Security Continuous Monitoring Shared Services can and will use its inherent vulnerability scanning ability to perform a self-assessment, this alone may not be sufficient. If IT Security Continuous Monitoring Shared Services was compromised or is malfunctioning it may not be able to detect issues within itself. This would not only undermine the continuous monitoring and diagnostics of IT Security Continuous Monitoring Shared Services but of all systems it monitors. Therefore, additional independent validation, verification, and assurance mechanisms should be considered for IT Security Continuous Monitoring Shared Services.

## **D.20 Accountability**

Ensuring all actions taken by a specific account is assigned to a single identity is essential to establishing accountability. All activities should be auditable and recorded into the audit log. Auditing will include who, what, where, and when any data was accessed. All IT Security Continuous Monitoring Shared Services System Administrators (SAs) will also have all their activities monitored in a manner that prevents the SAs from tampering with the records. A Security Officer will have the ability to audit SA behavior on the system. Administrators who are also users of the IT Security Continuous Monitoring Shared Services system will have separate accounts and use the privileged account only for administrative functions.

Retention of IT Security Continuous Monitoring Shared Services logs will take into account the requirements of individual Agencies. Some Agencies have unique regulatory requirements (i.e., logs related to a nuclear power plant will be kept for the duration of the life of the plant). Since IT Security Continuous Monitoring Shared Services only keep logs about its infrastructure, the

scope of these regulations and applicability to IT Security Continuous Monitoring Shared Services log retention requirements will be evaluated on a case-by-case basis.

## **D.21 Continuous Monitoring and Configuration Management Plan (CMP)**

Key Continuous Monitoring aspects that IT Security Continuous Monitoring Shared Services should address include:

- **Configuration Management:** A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout a system's lifecycle. IT Security Continuous Monitoring Shared Services will follow NIST's "Guide for Security-Focused Configuration Management of Information Systems," NIST SP 800-128, August 2011, in addition to NIST SP 800-53 Configuration Management (CM) family of CM security controls (CM-1 through CM-9), which will be outlined in the IT Security Continuous Monitoring Shared Services SSP
- **Configuration Management Plan:** A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems

## **D.22 Verification of SLA**

The SLA will define how all shared service-associated security principles will be monitored, verified, and tracked. The following will be addressed in the SLA:

- Define what protections/governance will be in place to monitor the Shared Service Provider
- Define who will monitor/govern the Shared Service Provider

## **D.23 Other SLA Considerations**

Appendix B lists common SLA guidelines. Some of the SLA-specific items are germane to IT Security Continuous Monitoring Shared Services security and have been stated throughout this document. SLA guidelines are presented to offer the IT Security Continuous Monitoring Shared Services community of interest guidance when creating legally-binding SLAs with Shared Service Providers. The guidelines are not exhaustive, but a basic foundation for further SLA dialogue with Shared Service Providers.

## **D.24 SLA Enforcement**

The SLA will define how disagreements and violations of the SLA will be resolved.

## **D.25 FISMA**

The current FISMA requirements are established in memorandums from the Office of The President listed here:

- MEMORANDUM FOR CHIEF INFORMATION OFFICERS “Security Authorization of Information Systems in Cloud Computing Environments,” from Steven VanRoekel, Federal Chief Information Officer, December 8, 2011
- MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES M-15-01 “Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices,” from Steven VanRoekel, Federal Chief Information Officer, October 3, 2014

## **D.26 IT Security Continuous Monitoring Shared Services Descriptions**

- Table 34 provides a set of IT Security Continuous Monitoring Shared Services user roles and a description of each role.

**Table 34: Role Descriptions**

<b>Role</b>	<b>Description</b>
Agency Portal User	A user designated by a Agency to have a need to know with authority to view the Agency asset and vulnerability data via a report or from the portal for that specific Agency
Shared Service Provider Portal User	A user designated by FNR and the Agencies to have a need to know to view the IT Security Continuous Monitoring Shared Services Provider asset and vulnerability data via a report or from the portal for the IT Security Continuous Monitoring Shared Services Provider enterprise only
Agency Third Party Portal User	A user designated by an Agency to have a need to know with authority to view the Agency's asset and vulnerability data via a report or from the portal for that specific Agency and only to the subset of assets outsourced to a specific third party
Agency Information Assurance (IA)/IT System Administrator Level-1	An SA that monitors and maintains IT Security Continuous Monitoring Shared Services components located at the Agency site(s). They can perform such activities as backup of component configuration and run diagnostics when needed; they cannot make configuration changes
IT Security Continuous Monitoring Shared Services IA/IT System Administrator Level-1	An SA that monitors and maintains IT Security Continuous Monitoring Shared Services components located at the Shared Service Provider's site(s). They can perform such activities as backups and run diagnostics when needed; they cannot make configuration changes
Agency Third Party IA/IT System Administrator Level-1	An SA that monitors and maintains IT Security Continuous Monitoring Shared Services components located at the Agency third party site(s). They can perform such activities as backup of component configuration and run diagnostics when needed; they cannot make configuration changes
Agency IA/IT System Administrator Level-2	An SA that can perform all the duties of a level-1 and also make configuration changes to IT Security Continuous Monitoring Shared Services component located at Agency site(s). They can also replace components if needed
IT Security Continuous Monitoring Shared Services IA/IT System Administrator Level-2	An SA at Shared Service Provider that can perform all the duties of a level-1 and also make configuration changes to IT Security Continuous Monitoring Shared Services component located at Shared Service Provider site(s). They can also replace components if needed
Agency Third Party IA/IT System Administrator Level-2	An SA that can perform all the duties of a level-1 and also make configuration changes to IT Security Continuous Monitoring Shared Services component located at Agency third party site(s) changes. They can also replace components if needed
Agency IA/IT Manager	A user designated by an Agency to have a need-to-know to view the Agency's asset and vulnerability data via a report or from the portal for that specific Agency. In addition they have the need to edit additional supplementary data for those assets/vulnerabilities

Role	Description
Shared Service Provider IA/IT Manager	A user designated by the Shared Service Provider to have a need-to-know to view the IT Security Continuous Monitoring Shared Services Provider asset and vulnerability data via a report or from the portal for IT Security Continuous Monitoring Shared Services Provider only data. In addition they have the need to edit additional supplementary data for those assets/vulnerabilities
Agency Third Party IA/IT Manager	A user designated by an Agency to have a need-to-know to view the Agency's asset and vulnerability data via a report or from the portal for that specific Agency, and only to the subset of assets outsourced to a specific third party. In addition they have the need to edit additional supplementary data for those assets/vulnerabilities
Agency IA/IT Metrics Management	A user who can view high level tracking and monitoring metrics or related information to IT Security Continuous Monitoring Shared Services
Shared Service Provider IA/IT Metrics Management	A user at the Shared Service Provider who can view O&M and low level tracking and monitoring metrics or related information to IT Security Continuous Monitoring Shared Services