



**IT Security Procedural Guide:
Information Security Continuous
Monitoring (ISCM) Strategy & Ongoing
Authorization (OA) Program
CIO-IT Security-12-66**

Revision 3

April 23, 2020

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Initial Release – June 24, 2019				
1	Desai	Updates necessary to support requirements within OMB M-14-03.	OMB M-14-03	Throughout the document
2	Desai, Davis	Updates necessary to support NIST SP 800-53 R4 and addition of Continuous Monitoring Performance Metrics.	NIST SP 800-53 R4	Throughout the document
Revision 1 – May 11, 2017				
1	Dean/Klemens	Reformatted to current style and structure. Removed database scanning requirements.	Update to the reflect updates to GSA CIO Order 2100.1 and CIO-IT Security-06-30.	Throughout the document
Revision 2 – October 10, 2017				
1	Dean/Feliksa/Klemens/Desai/Valenzuela	Restructured document to reflect current GSA ISCM strategy and program.	Updated to align with GSA's use of Federal CDM tools and Federal guidance on ISCM and ongoing authorization. Incorporated Executive Order 13800 and NIST Cybersecurity Framework.	Throughout the document
Revision 3 – April 23, 2020				
1	Chinn/Normand	Revised and restructured document: <ul style="list-style-type: none"> • Added OA Team role • Distinguished ISCM Strategy from OA Program • Revised onboarding, performance metrics, and OA maintenance processes • Added Control Responses for specific NIST controls • Revised ISCM controls 	Updated to align with the FY20 changes for the ISCM program.	Throughout the document

APPROVAL

IT Security Procedural Guide: Information Security Continuous Monitoring (ISCM) Strategy and Ongoing Authorization (OA) Program, CIO-IT Security-12-66, Revision 3, is hereby approved for distribution.

X

DocuSigned by:
Bo Berlas

FD747096404544F...

Bo Berlas

Chief Information Security Officer (CISO)

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

1	Introduction	1
1.1	Purpose.....	1
1.2	Scope	1
1.3	Policy	1
2	ISCM Roles and Responsibilities	2
2.1	The Chief Information Security Officer (CISO).....	2
2.2	Authorizing Official (AO).....	2
2.3	System Owner (SO).....	3
2.4	OA Information Systems Security Manager (ISSM).....	3
2.5	OA Information Systems Security Owner (ISSO)	3
2.6	OCISO Policy and Compliance Division (ISP)	4
2.7	OA Team	4
3	ISCM Strategy	4
4	The OA Program	5
4.1	Onboarding Systems into Ongoing Authorization.....	5
4.1.1	<i>Prerequisites for Requesting Ongoing Authorization</i>	<i>6</i>
4.1.2	<i>OA Kickoff Meeting.....</i>	<i>6</i>
4.1.3	<i>OA Checklist.....</i>	<i>7</i>
4.1.4	<i>OA Onboarding Assessment Report (OAR).....</i>	<i>7</i>
4.1.5	<i>Onboarding Approval Meeting (OAM)</i>	<i>7</i>
4.1.6	<i>OATO Letter</i>	<i>8</i>
4.2	Maintaining Ongoing Authorization.....	8
4.2.1	<i>Automated Reporting and ISSO Checklist.....</i>	<i>8</i>
4.2.2	<i>Biannual Performance Metric Review (PMR).....</i>	<i>8</i>
4.2.3	<i>OA Non-Compliance</i>	<i>10</i>
4.2.4	<i>Handling Incidents or Significant Change within the OA Program.....</i>	<i>10</i>
5	Continuous Diagnostics and Mitigation (CDM) Tools	11
5.1	Automation Capabilities Supporting ISCM	11
5.2	GSA Security Capabilities.....	12
5.2.1	<i>Manage Assets</i>	<i>13</i>
5.2.2	<i>Hardware Asset Management (HWAM)</i>	<i>13</i>
5.2.3	<i>Software Asset Management (SWAM)</i>	<i>13</i>
5.2.4	<i>Configuration Settings Management (CSM)</i>	<i>14</i>
5.2.5	<i>Vulnerability Management (VUL).....</i>	<i>14</i>
5.2.6	<i>Manage Events.....</i>	<i>15</i>
Appendix A – ISCM Controls		20
Appendix B – References.....		27

Table of Figures and Tables

Figure 4-1. Ongoing Authorization Steps6
Figure 5-1. ISCM/CDM Capability Wheel12
Table A-1: OA Program Common Control Responses20
Table A-2: Automated ISCM Controls24
Table A-3: Process-based ISCM Controls26

Note: Hyperlinks in this guide are provided as follows:

- Appendix B References - This section contains hyperlinks to Federal Regulations/Guidance and to GSA webpages containing GSA policies, guides, and forms.
- In running text - Hyperlinks will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in Appendix B. For example, Google Forms, Google Docs, and websites will have links.

Note: It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

Information Security Continuous Monitoring (ISCM) as defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, “*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*,” is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Per NIST SP 800-137, “An ISCM program is established to collect information in accordance with preestablished metrics, utilizing information readily available in part through implemented security controls,” and “Organizations’ security architectures, operational security capabilities, and monitoring processes will improve and mature over time to better respond to the dynamic threat and vulnerability landscape. An organization’s ISCM strategy and program are routinely reviewed for relevance and are revised as needed to increase visibility into assets and awareness of vulnerabilities. This further enables data-driven control of the security of an organization’s information infrastructure, and increase organizational resilience.”

The General Services Administration’s (GSA) ISCM Strategy and Ongoing Authorization (OA) Program, as described in NIST SP 800-137, will facilitate a migration from compliance-driven risk management to data-driven risk management. This move will provide GSA with the information necessary to support risk response decisions, security status information, and ongoing insight into security control effectiveness.

1.1 Purpose

The purpose of this guide is to define the GSA ISCM Strategy and the approach for implementing and maintaining an OA Program. The establishment of an OA process model for information systems accepted into the agency’s OA Program. The guide provides GSA Federal employees and contractors with significant security responsibilities, and other IT personnel involved in implementing the ISCM Strategy and OA Program requirements.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in implementing and maintaining GSA’s ISCM Strategy and OA Program. All GSA IT Systems are a part of GSA’s overall ISCM strategy and systems in OA must adhere to the requirements of the OA Program.

1.3 Policy

GSA CIO 2100.1, “*GSA Information Technology (IT) Security Policy*,” contains the following policy statements regarding requirements related to the ISCM program.

Chapter 3, Policy for Identify Function, states:

Governance.

i. AOs must ensure risk assessments are performed and documented as part of A&A activities IAW GSA CIO-IT Security-06-30 before a system is:

- (1) Placed into production;*
- (2) When significant changes are made to the system;*

- (3) At least every three (3) years; OR
 (4) Via continuous monitoring based on continuous monitoring plans reviewed and accepted by the GSA CISO.

I. Extension of a system's current ATO for a period not to exceed one year (365 days) may only be requested under one of the following conditions. The system must continue to maintain its complete set of A&A documentation (e.g., System Security Plan, Contingency Plan, POA&Ms). All actions to satisfy the conditions below must be completed within the extension period (i.e., no longer than 12 months).

- (1) Transitioning to ongoing authorization;

Chapter 5, Policy for Identify Function, states:

Security continuous monitoring.

a. OCISO will implement continuous monitoring of systems using Continuous Diagnostics and Mitigation (CDM) and other enterprise security tools as described in GSA CIO-IT Security-12-66: Information Security Continuous Monitoring.

2 ISCM Roles and Responsibilities

There are many roles and responsibilities associated with implementing and managing an effective ISCM strategy and OA Program. The roles and responsibilities identified in this section have been paraphrased from the [ISCM Responsible, Accountable, Consulted, Informed \(RACI\) Guide](#) and are in addition to the agency's Security Roles and Responsibilities defined by GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy."

2.1 The Chief Information Security Officer (CISO)

Responsibilities include the following:

- Developing, implementing, and maintaining an agency-wide GSA ISCM Strategy and OA Program.
- Reporting to the GSA CIO on the implementation and maintenance of the GSA's OA Program.
- Acquiring or developing and maintaining automated tools to support the ISCM Strategy and OA Program.
- Providing training on the organization's ISCM Strategy, OA Program and operational process.
- Providing support to information system OAs and system owners on how to implement the OA Program requirements for their systems.
- Accepting the risk of operating GSA information systems under their purview, including having implemented required continuous monitoring controls and settings in accordance with GSA and Federal policies and requirements.

2.2 Authorizing Official (AO)

Responsibilities include the following:

- Accepting the risk of operating GSA information systems under their purview, including having implemented required continuous monitoring controls and settings in accordance with GSA and Federal policies and requirements.
- Ensuring a plan of action and milestones (POA&M) item is established and managed to address any controls required as a part of continuous monitoring that have not been fully implemented.
- Reviewing continuous monitoring reports/dashboard and making a risk-based determination on a system's ongoing authorization status.
- Determining whether a breach or information system change requires an event-driven reauthorization.
- Ensuring the organization's OA Program is applied with respect to a given information system.

2.3 System Owner (SO)

Responsibilities include the following:

- Ensuring required continuous monitoring controls and settings are in place and operating in accordance with GSA and Federal policies and requirements.
- Maintaining required continuous monitoring documentation.
- Reviewing continuous monitoring reports/dashboard and responding, as necessary, to maintain a system's ongoing authorization.
- Assisting in determining whether a breach or information system change requires an event-driven reauthorization.

2.4 OA Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Assisting in the OA Program's Biannual Performance Metric review requirements.
- Monitoring and supporting the resolution of POA&Ms to mitigate system vulnerabilities regarding continuous monitoring controls for all systems under their purview.
- Coordinating with ISSOs on information systems' monthly, quarterly, and annual security requirements.
- Coordinating with OA ISSOs to establish and manage ISCM processes and procedures (e.g., reviewing and coordinating ISCM reports/dashboards, reviewing events to determine if an event-driven reauthorization is required, etc.) Performs drafting of OATO letter, for AO and CISO approvals.

2.5 OA Information Systems Security Owner (ISSO)

Responsibilities include the following:

- Ensuring required continuous monitoring controls and settings are in place and operating in accordance with GSA and Federal policies and requirements.
- Developing and maintaining POA&Ms, as necessary, regarding continuous monitoring controls for assigned systems.
- Verifying the maintenance of (or maintaining) required continuous monitoring documentation.
- Maintaining compliance with continuous monitoring processes and procedures (e.g., inventories are up to date, reports are submitted).

- Assisting in remediation activities as necessary to maintain ongoing authorization.
- Collaborating with the OA Team on completing assigned OA Checklists and Biannual Performance Metric Review (PMR) requirements.

2.6 OCISO Policy and Compliance Division (ISP)

Responsibilities include the following:

- Acting as custodian of the Archer Governance, Risk, and Compliance (GRC) tool and the CDM Program Management Office (PMO).
- Facilitating OA Program reporting requirements to CISO, AOs, and System Owner.
- Managing the OA Program system prioritization list.
- Providing formal ISCM Strategy and OA Program guidance.
- Providing security management oversight of the OA Program and the defined Performance Metrics.

2.7 OA Team

Responsibilities include the following:

- Architecting, reviewing, and defining various OA Program processes for efficiency, compliance and accuracy.
- Managing the OA Program onboarding processes of new information systems.
- Conducting Biannual PMRs of all systems accepted into the OA Program with the assigned OA ISSOs.
- Facilitating OA Program reporting requirements to the OA ISSM.
- Conducting OA Program reporting requirements.

3 ISCM Strategy

The GSA ISCM Strategy leverages both manual and automated processes that involve the monitoring of a system's NIST security controls. The strategy will ensure all key information security controls are periodically assessed for effectiveness. Monitoring activities are biased towards controls with the greatest impact. GSA's ISCM Strategy will expand and mature over time to ensure improvement. Security control analysis, monitoring and assessment frequencies of continuous monitoring and verification requirements will change IAW with GSA's needs. The OCISO will regularly review the ISCM Strategy to ensure it sufficiently supports the GSA's requirements to operate systems within acceptable risk tolerance levels, identify ways to improve organizational insight into security posture, effectively support informed risk management decisions, and improve GSA's ability to respond to known and emerging threats.

GSA's ISCM organizational strategy leverages its deployment of Continuous Diagnostics and Mitigation (CDM) and other Enterprise Security Management tools. GSA's tool stack facilitates near real-time risk management of GSA information systems. Every GSA IT system benefits from GSA's ISCM risk management processes based on the continuous monitoring of vulnerabilities, threats, and actions taken to reduce, mitigate, or eliminate them. GSA has implemented its ISCM strategy leveraging regular vulnerability scanning activities and the requirement to maintain Security Assessment and Authorization

(A&A) documents in an “as-is” state. In addition to the automation provided by the tool stack, the GSA’s ISCM strategy leverages manual processes defined by:

- CIO-IT Security-04-26, “*FISMA Implementation Guide*”
- CIO-IT Security-06-30, “*Managing Enterprise Risk*”
- CIO-IT Security-09-44, “*Plan of Action and Milestones*”
- CIO-IT Security-17-80, “*Vulnerability Management Process*”
- CIO-IT Security-18-90, “*Information Security Program Plan*”
- CIO-IT Security-19-95, “*Security Engineering Architectural Reviews*”
- CIO-IT Security-19-101, “*External Information System Monitoring*”

In addition to the ISCM Strategy, GSA has established an Ongoing Authorization (OA) Program with defined information system qualifying requirements. The OA Program objective has been defined to achieve Ongoing Authorization to Operate (OATO) for GSA managed information systems. The Office of the Chief Information Security Officer (OCISO) and the system’s Authorizing Official (AO) accept an information system into the OA Program based on it meeting the program’s prerequisites, its usage of enterprise security tools, and its compliance with the requirements of the program. Upon acceptance for OATO, the system will not require re-authorization every three years, however an event driven re-authorization will be required if the system:

- Has a significant change as defined in NIST SP 800-37, Appendix F.
- Has a security breach that impacts the security posture of the system.

GSA information systems that do not meet the qualifying requirements for transitioning into the OA Program, must follow one of the A&A processes defined by CIO-IT Security-06-30.

4 The OA Program

Information collected through the OA Program supports OA decisions. The overall program strategy ensures all key information security controls are periodically assessed for effectiveness, at a higher frequency than the agency’s traditional 3-year ATO processes. As the OA Program at GSA matures and grows, the OCISO will revise the program, as appropriate, to ensure systems’ security posture can be monitored regularly, continue to operate within GSA’s risk tolerance, and can quickly respond to emerging threats.

The primary function of the OA Program is to onboard eligible GSA information systems into the program. OA provides a more frequent view into the security posture of the on boarded systems. The OA Program uses biannual reviews to ensure all responsible parties are executing their responsibilities according to the defined OA Program requirements and system OATOs are maintained.

4.1 Onboarding Systems into Ongoing Authorization

Before an information system can become part of the OA Program, it must go through a onboarding process to ensure the system has met all CIO-IT Security-06-30 and the OA Program requirements. The following OA subsections of this guide elaborate on each of the major steps involved in the OA onboarding processes shown in Figure 4-1.



Figure 4-1. Ongoing Authorization Steps

4.1.1 Prerequisites for Requesting Ongoing Authorization

GSA information systems must meet the following requirements before it can be considered for onboarding into the OA Program. These prerequisites are part of the pre-assessment conducted by the OA Team and determine the eligibility of the system to receive an OATO.

- The information system must have had all of its NIST SP 800-53 security controls for its applicable FIPS 199 level, and any additional controls required by the GSA CISO assessed within the past 18 months and issued an ATO.
- The information system must have deployed GSA’s enterprise ISCM tools, based on applicable system requirements, defined within the [GSA ISCM Enterprise Security Management Tools](#).

4.1.2 OA Kickoff Meeting

After a candidate system has met the prerequisites listed above, an OA Kickoff meeting will be scheduled with all relevant stakeholders. The meeting is arranged and led by the OA Team. It serves to clearly identify the OA Program’s onboarding tasks responsibilities, and schedule. The kick off agenda will include, at minimum:

- Review of the OA Onboarding Assessment Report (OAR)
- Review of the OA Checklist Template
- Review of the OA Controls (see [Appendix A](#))
- Review of the OATO Letter Template
- Scheduling of the next OA Review Meeting
- High level assessment of showstopper controls as identified by CIO-IT Security-06-30
- Creation of a System Document Repository for automated CDM scans (BigFix, TSC, Netsparker, etc.)
- Identification of all required security documentation, including (as attachments):
 - System Security Plan
 - Plan of Action and Milestones (POA&M)
 - FISMA Self-Assessment Results
 - OS Vulnerability scan results
 - Unauthenticated Web Vulnerability scan results (as applicable)
 - Authenticated Web Vulnerability scan results (as applicable)
 - Penetration Test Results (as applicable)
 - Hardware Asset Inventory Report generated by automated tool
 - Software Asset Inventory Report generated by automated tool
 - Configuration Compliance scan results

- Configuration Management Plan
- IT Contingency Plan
- IT Contingency Plan Test Results
- Incident Response Plan
- Incident Response Plan Test Results
- Privacy Threshold Analysis or Privacy Impact Assessment (PIA) (as applicable)

After the OA Kickoff meeting, all attendees will understand their role and responsibilities regarding the OA Program requirements and the onboarding schedule. The OA Team will work with the OA ISSO and stakeholders to address any OA questions and the scheduling of follow-on meetings.

4.1.3 OA Checklist

The [OA Checklist](#) is completed by the OA Team in coordination with the system team members (SO, OA ISSO and OA ISSM). It serves as evidentiary documentation detailing the compliance status for all relevant OA controls of the assessed candidate system identified during the onboarding review process. The OA checklist results are utilized to represent the system's readiness for the system's AO and CISO onboarding approvals and entry into the OA Program.

The OA checklist reviews five main security areas including ISCM/CDM Tools, Vulnerability Management, Configuration Compliance, Critical Security Controls and Security Documentation. Each category has several requirements that are rated as Fully Satisfied (red), Partially Satisfied (yellow) or Not Satisfied (red). The OA Team records detailed assessment results and links to system specific evidence artifact(s) for each requirement. Not all areas or checks are showstoppers (as identified by CIO-IT Security-06-30). ISCM Program requirements not rated as Fully Satisfied can delay or even remove a system from the ISCM program eligibility. This decision is made after the completed OA Checklist and OAR are reviewed.

4.1.4 OA Onboarding Assessment Report (OAR)

The OA Team and the system's OA ISSO are responsible for the creation of the OAR. The OAR addresses the required actions taken to maintain a compliant status within the OA Program. It is created for the initial assessment of an information system and provides evidence that the system has met all requirements for onboarding into the OA Program. Additionally, the OAR is a reference document that can be used as a resource showing the strategy and requirements for maintaining the OATO by the SO, OA ISSO, and OA ISSM.

Functionally, the OAR amounts to a Security Assessment Report (SAR) for the OA Program. It contains an executive summary, an overview of the status of the system's ISCM security controls, a summary report of the OA Checklist, and an OA Program recommendation. Along with the OATO Letter (section 4.1.6) the OAR is the key document for identifying if a system should or should not be allowed to progress into the OA Program. The OAR is completed by the OA Team and the results concurred with by the System Owner, OA ISSO, and OA ISSM.

4.1.5 Onboarding Approval Meeting (OAM)

An OAM is scheduled after the OA Checklist and OAR have been completed. The meeting is led by the OA Team and includes the system team and personnel from ISP. In this meeting an overview of the results of the OA Checklist and OAR are presented, and a final recommendation will be made by the ISP Director. The meeting will identify any contingent actions that must be completed before the system is

onboard ready. The OAM may result in a system being placed on hold to resolve any unsatisfied OA Program requirements. At the end of the OAM, the OA Team will provide attendees with a summary of the meeting and identify any assigned actions or next steps.

4.1.6 OATO Letter

An [OATO Letter](#) is prepared by the OA ISSM in coordination with the OA ISSO and the OA Team, and is sent to the CISO and AO for their approval and concurrence. Once the OATO Letter has been signed, it will be forwarded to the OA Team and ISP (ispcompliance@gsa.gov), the system OA ISSO is required to upload the signed OATO Letter to the Archer GRC A&A Repository.

4.2 Maintaining Ongoing Authorization

After a system has been on boarded into the OA Program, there are little to no changes in the day to day O&M activities performed by the system's OA ISSO and OA ISSM. They will remain the primary security point of contact and liaison for their assigned system. They are responsible for monitoring, reporting upon, and ensuring the accuracy of the system's automated reports, based upon the system's inventory requirements. They are required to maintain their system's security documents and perform periodic reviews based upon their defined frequencies. They are required to monitor and manage the timely completion of system POA&Ms.

Though the daily operations are similar, the reporting and review mechanics of a system's ongoing authorization are different. Instead of a 3 year ATO cycle, systems in the OA program are subject to Biannual PMRs. After each PMR is completed, the results are presented to the CISO and the system's AO who make a risk based decision regarding continuing the system's OATO.

4.2.1 Automated Reporting and ISSO Checklist

In support of the Biannual PMRs, OA ISSOs must perform the following actions for their systems In the OA Program:

- Generate automated reports from the CDM tools and review them for accuracy. The automated reports must be filed in the system's OA documentation repository that was created during the Kickoff Meeting (section [4.1.2](#)). It is essential the reports be maintained to provide an accurate historical view of the system.
- Complete the Archer GRC ISSO Checklists for their systems within the allotted timeframe specified for each checklist. Incomplete or late checklist items will be identified during a system's Biannual PMR.

4.2.2 Biannual Performance Metric Review (PMR)

Biannual PMRs are an OA Program feedback mechanism. PMRs are used to ensure GSA information systems with an OATO continue to operate in accordance with the OA program's requirements. The OCISO will provide Biannual PMR status updates to the AOs on their systems' performance within the OA Program. The PMR tracks submissions of required OA Program deliverables to the OCISO and the continued effectiveness of CDM and GSA ISCM Enterprise Security Management automated capabilities for each information system (as applicable).

4.2.2.1 Biannual PMR Report

After a system is granted an OATO and is integrated into the OA Program, the system must meet the agency's defined performance metrics, as identified in the Biannual Performance Metric Review (PMR) Report template (Google Sheet will be provided by the OA Team). The Biannual PMR Report template will be updated as new performance metrics are identified, per each FY. Any updates will be communicated to OA ISSOs and OA ISSMs with systems in the OA Program prior to the first scheduled PMR. The performance metrics results are utilized to provide the CISO and AOs a holistic view of the security posture of the systems within the OA Program. The performance measures include areas covered by security automation domains and manual deliverables. Metrics have been defined to align with the information security goals for each of the following domains:

- Hardware Asset Management
- Software Asset Management
- Configuration Settings Management
- Vulnerability Management
- Event Management
- Periodic Deliverables
- Annual Deliverables

Each performance metric has been evaluated by ISP and assigned reporting status levels. Each level is based upon the metric's security risk impact, per the OA Program's reporting requirements. The metric reporting status levels are color coded:

- Red – identifies the metric is Not Satisfied
- Yellow – identifies the metric is Partially Satisfied
- Green – identifies the metric is Fully Satisfied

The Biannual PMR report includes an executive level dashboard and summarizes the performance metric information captured during the system's PMR. It provides trending information upon completion of both FY PMRs. The trending information provides ISP, CISO, and the AOs the ability to see the progress or regression of a system within the OA Program.

The Biannual PMR report is completed by the OA Team in coordination with the system OA ISSO, OA ISSM and ISP. If the review indicates any partially or non-compliant metrics, the OA Team works with the system's security team to verify the findings. On a case-by-case basis, the OA Team will allow for remediation actions to be performed to improve PMR metrics before completing their review. As system PMRs are completed they are sent to the ISP Director for review. Once all the PMRs are completed, the findings are analyzed including identifying any common threads. Based on this analysis, a presentation is prepared for the CISO highlighting significant system specific findings, any common threads, and any recommendations regarding the OA Program or specific systems.

4.2.2.2 OCISO Reviews

The OCISO uses the Biannual PMR reports to evaluate a system's performance within the OA Program, and to measure the effectiveness of the implemented OA continuous monitoring controls, and security automation domains. Biannual status reports using the defined performance metrics are sent to the AOs and the CISO, copied are the OA ISSMs, OA ISSOs, and system owners for performance tracking.

Performance metrics summarize the system's overall security posture and will serve as a means for the AO and CISO to make a risk based decision on maintaining the system's OATO.

Based on a review of the Biannual PMR Reports, the CISO and AO will determine if a system's previously approved OATO is being effectively implemented and maintained. If the AO and the CISO determine that the system's OATO is not effectively being maintained, the System Owner/Program Manager, OA ISSM, and OA ISSO will be notified of the observed deficiencies. The system will be identified as OA Non-Compliant and the system team will be provided with a timeframe to address the identified OA Program deficiencies.

4.2.3 OA Non-Compliance

If a system is identified as OA Non-Compliant the timeframe allotted to correct deficiencies will be considered a system's probation period within the OA Program. If the observed deficiencies have been fully addressed the system retains its OATO. If the observed deficiencies are not fully addressed during the probation period, the system team will be required to present their progress in correcting deficiencies to the CISO and AO for their review and consideration. Based on their review, the AO and CISO may determine the system:

- Has made adequate progress addressing deficiencies and there is an acceptable plan to address remaining issues. The system retains its OATO.
- Has not made adequate progress addressing deficiencies or the plan to address remaining issues is not adequate. The system will be required to exit the OA Program and complete a standard A&A defined in CIO-IT Security-06-30 to achieve a new ATO.

4.2.4 Handling Incidents or Significant Change within the OA Program

Information systems undergo frequent changes to hardware, software, firmware, or supporting networks during the system's life cycle. Such changes are typically addressed via configuration management and control processes ensuring all proposed changes are tested to observe the effects and impact of the change, and are approved prior to implementation, thereby minimizing the risk of adverse results. All system changes, regardless of size, should follow the formal, documented change management process for the system, and that change management process should contain the steps for completing a Security Impact Analysis on any proposed change. Not all system changes will have an impact on security, and the OA ISSO should be involved in the analysis prior to the change to determine the risks the change presents and recommend an appropriate course of action.

Significant changes must be coordinated with the OCISO prior to a final determination being made and a course of action agreed upon for handling the change.

Examples of significant changes to an information system include:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Installation of a new or upgraded hardware platform;
- Modifications to cryptographic modules or services; or
- Modifications to security controls.

Examples of significant changes to the environment of operation include:

- Moving to a new facility;
- Adding new core missions or business functions;
- Acquiring specific and credible threat information that the organization is being targeted by a threat source; or
- Establishing new/modified laws, directives, policies, or regulations;
- Virtualization of the system;
- Addition of telecommunication capability; or
- Moving the system to the “Cloud.”

Incidents or significant changes regarding a system may require its reauthorization. The reauthorization process differs from the initial authorization inasmuch as the AO can initiate: a complete zero-base review of the information system or common controls; or a targeted review based on the type of event that triggered the re-authorization, the assessment of risk related to the event, and the organizational risk tolerance. Re-authorization is a separate activity from the ongoing authorization process, though security- and privacy-related information from the organization’s OA Program may still be leveraged to support re-authorization.

5 Continuous Diagnostics and Mitigation (CDM) Tools

The overall focus in utilizing CDM tools as part of the GSA ISCM Strategy and OA Program is to provide sufficient information about a GSA managed information systems security control effectiveness and security status to allow GSA management to make informed, timely security risk management decisions aimed at supporting system’s authorizations.

5.1 Automation Capabilities Supporting ISCM

NIST SP 800-53 defines a security capability as: “A construct that recognizes that the protection of information being processed, stored, or transmitted by information systems, seldom derives from a single safeguard or countermeasure (i.e., security control). In most cases, such protection results from the selection and implementation of a set of mutually reinforcing security controls.”

NIST SP 800-53, Revision 4 further notes that:

- Failure of a single control or in some cases, the failure of multiple controls, may not affect the overall security capability needed by an organization.
- Employing the broader construct of security capability allows an organization to assess the severity of vulnerabilities discovered in its information systems and determine if the failure of a particular security control (associated with a vulnerability) or the decision not to deploy a certain control, affects the overall capability needed for mission/business protection.

Using this concept of security capability, the DHS CDM program defines and groups ISCM capabilities into 4 families and 15 security capabilities as follows:

1. Manage Assets - What assets do we have and do we have the assets we need?
2. Manage Accounts for People and Services - Do the right people have the right access to do the right things?
3. Manage Events - Are we prepared for and can we respond to incidents?
4. Manage Security Lifecycle - Are we considering security throughout the lifecycle of our assets?

Figure 5.1 portrays the DHS CDM Program's four families and fifteen security capabilities, the figure is also available at the US Computer Emergency Readiness Team (CERT) [CDM website](#).

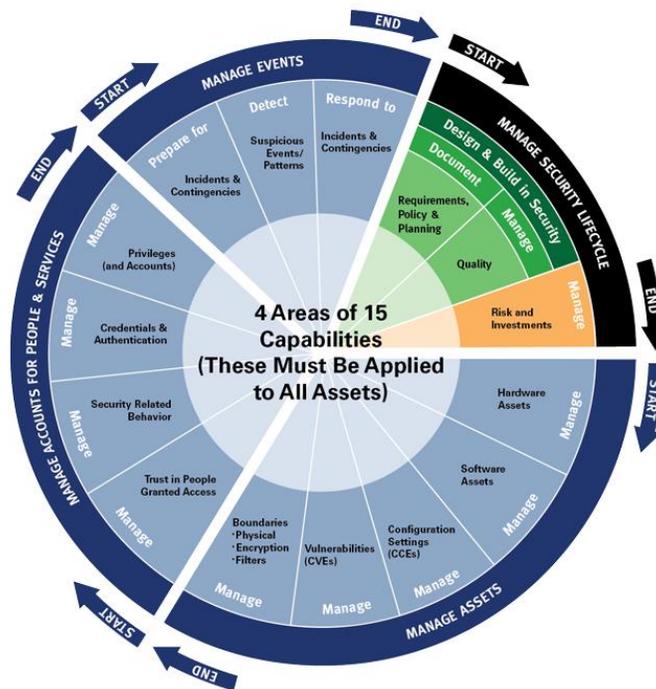


Figure 5-1. ISCM/CDM Capability Wheel

Four of the five capabilities are provided within Phase 1 of DHS' CDM program:

- HWAM - Hardware Asset Management
- SWAM - Software Asset Management
- CSM - Configuration Settings Management
- VUL - Vulnerability Management

5.2 GSA Security Capabilities

This section identifies the security capabilities supporting ISCM/CDM that have been implemented by GSA. In addition to the current ISCM processes for monitoring controls, the GSA Enterprise CDM tools will provide inherited controls for HWAM with ForeScout CounterACT/SecureConnector and IBM Bigfix, SWAM and Security Configuration Compliance (as a part of Configuration Settings Management) with IBM BigFix, White/Blacklisting with Bit9, and Vulnerability Scanning with Tenable. As GSA's Continuous Monitoring program matures over time, additional capabilities will be added.

System Owners, OA ISSMs, and OA ISSOs are responsible for ensuring that all ISCM controls are implemented. For inherited controls, including the common portion of hybrid controls, their responsibility is to ensure the providing system agrees the system is inheriting the control. For technical controls satisfied by the implementation of enterprise tools, they must ensure the tools are deployed and operating as intended by the enterprise.

5.2.1 Manage Assets

The Manage Assets family and its capabilities act as a foundation for the other security automation domains. The primary objective of the Manage Assets family is to manage hardware and software inventories and the security (configuration and vulnerabilities) of the inventoried assets in the organization.

5.2.2 Hardware Asset Management (HWAM)

Purpose - Maintain an asset inventory of authorized hardware assets/devices allowed to connect to a network. Identify unauthorized and unmanaged devices that are likely to be used by attackers as a platform from which to extend compromise of a network. The Hardware Asset Management capability ensures that a hardware inventory and supporting processes are in place to confirm that only authorized hardware can be added to a network.

NIST SP 800-53 Controls - Controls related to hardware asset management include but are not limited to CM-8, CM-8(1), CM-8 (2), CM-8(3), CM-8(4), CM-8(5), and CM-8(7).

Target Attack Vectors - Attackable Hardware Devices including all IP-addressable devices (or equivalent) on a network. Attackers continually scan for hardware systems that they can exploit to gain control of and use to access other devices and data. Typically, the most exposed devices are unauthorized or unmanaged.

Implementation Approach - Maintain a list of authorized hardware and who manages it. Treat other hardware on the network as a defect. Remove, authorize/assign, or accept risk of unauthorized hardware assets. This can be accomplished via a combination of system configuration, network management, and license management tools, or with a special-purpose tool. Employ both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic.

GSA Enterprise Tool(s) - GSA uses a combination of agent-based, agentless (discovery scans), network management, IT Service Management, and IP Management solutions to implement hardware asset management. Please refer to the [GSA Enterprise Continuous Monitoring Tools](#) for a detailed list of tools used to implement hardware asset management for different asset categories in the GSA environment.

5.2.3 Software Asset Management (SWAM)

Purpose - Maintain an asset inventory of approved software. Identify unauthorized software on devices that are likely to be used by attackers as a platform from which to extend compromise of a network.

NIST SP 800-53 Controls - Controls related to software asset management are CM-2, CM-2(1), CM-2 (2), CM-7(4), and CM-7(5).

Target Attack Vectors - Software products (e.g., MS-Word) and executables (individual program files). Identify executables by their digital fingerprint.

Implementation Approach - Maintain a list of authorized software at both the product and executable level. Treat other software actually on network as a defect. In other words, deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and

prevents execution of all other software on the system. Remove, authorize/assign, or accept risk of unauthorized software.

GSA Enterprise Tool(s) - GSA uses a combination of agent-based solutions (e.g. BigFix, MaaS360, and Tenable Security Center) to implement software asset management. GSA also uses application whitelisting tools (e.g., Bit9) to prevent software execution in accordance with (IAW) the list of authorized software programs. The [GSA Enterprise Continuous Monitoring Tools](#) provides a detailed list of tools used to implement software asset management for different asset categories in the GSA environment.

5.2.4 Configuration Settings Management (CSM)

Configuration settings management is primarily focused on the configuration status of computing devices and software across an enterprise. It involves determining compliance by collecting detailed information about specific configuration settings and comparing that data against an organization's standard configuration. GSA has established a series of hardening guides for commonly used technologies (e.g., operating systems, database management systems) with defined standard configuration settings to which existing and newly added assets will be measured against. Hardening guides are available on the [IT Security Technical Guides and Standards](#) webpage. CDM tools (e.g., BigFix, Tenable) will be used for measuring configuration compliance and can support determining root causes for misconfiguration and implementing corrections.

Purpose - Manage configuration settings, monitor changes to settings, collect setting status, and restore settings as needed. Identify configuration settings (CCEs) on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network. Configuration settings are often used as a means to support other capabilities, such as blocking certain software and/or granting/denying privilege(s).

NIST SP 800-53 Controls - Controls related to configuration settings management are CM-6, CM-6 (1), CM-7, CM-7(1), CM-7(2), CM-7(4), and CM-7(5).

Target Attack Vectors - Individual Configuration settings, or groups of such settings.

Implementation Approach - Maintain a list of authorized settings/configuration benchmarks for software product categories such as Operating System, Servers (Web, Email, Application, DNS, Directory, etc.), networking devices (Routers, Switches), multifunction peripheral devices, desktop applications, web browser, etc. Remove, authorize/assign, or accept risk for unauthorized settings.

GSA Enterprise Tool(s) - GSA will leverage existing ISCM enterprise security and CDM tools including BigFix and Tenable to provide asset management for software products installed on applicable endpoints for centrally managing, applying and verifying configuration settings. The [GSA Enterprise Continuous Monitoring Tools](#) Google Sheet provides a detailed list of tools used to implement configuration compliance.

5.2.5 Vulnerability Management (VUL)

Vulnerability management is concerned with understanding the security posture with respect to known vulnerabilities. It involves collecting information regarding vulnerabilities and patch levels of assets across the enterprise.

5.2.5.1 Vulnerability Detection

Purpose - Identify vulnerabilities (CVEs) on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

NIST SP 800-53 Controls - Controls related to vulnerability management of known vulnerabilities and patches, and remediating flaws or mitigating vulnerabilities are RA-5, RA-5(1), SI-2, SI-2(2), and SI-2(3).

Targets Attack Vectors - Individual CVEs, or groups of such CVEs.

Implementation Approach - The [National Vulnerability Database](#) (NVD) provides a library of vulnerabilities mapped to vulnerable software. Poor coding practices can manifest as vulnerabilities that are discovered and assigned a CVE. Upgrade the software to newer, non-vulnerable versions, apply appropriate patches, modify the code to eliminate or mitigate vulnerabilities, or accept the risk.

GSA Enterprise Tool(s) - GSA uses the Tenable enterprise vulnerability scanning tool to identify known vulnerabilities and will leverage the CDM BigFix tool as an enterprise patch management solution to deploy latest patches for operating systems and applications. The [GSA Enterprise Continuous Monitoring Tools](#) Google Sheet provides a detailed list of tools used to implement vulnerability and patch management.

5.2.5.2 Malware Detection

Purpose - Provide the ability to identify and report on the presence of viruses, Trojan, spyware, or other malicious code on or destined for a target system.

NIST SP 800-53 Controls - Controls related to identifying unauthorized or malicious code and employing protection mechanisms against malicious code execution, and controls related to detect unauthorized changes to software to ensure software and information integrity: SI-3, SI-3(1), SI-7, and SI-7 (3).

Targets Attack Vectors - End-users and organizations via web browsing, email attachments, endpoint devices such as workstations, mobile devices, executables, etc.

Implementation Approach - Employ malware detection tools and mechanisms at information system entry and exit points (e.g., firewalls, email servers, Web servers, proxy servers, remote access servers) and at endpoint devices (e.g., workstations, servers, mobile computing devices) on the network to detect and remove malicious code. Malware detection mechanisms can be configured to perform periodic scans of information systems, as well as real-time scans of files from external sources as the files are downloaded, opened, or executed IAW organizational security policy.

GSA Enterprise Tool(s) - GSA uses centrally managed integrity verification tools and application whitelisting tools that detects and prevents/blocks malicious code execution. GSA also employs Antivirus tools on workstations, servers and mobile devices. The [GSA Enterprise Continuous Monitoring Tools](#) Google Sheet provides a detailed list of tools used to implement malware detection.

5.2.6 Manage Events

The Manage Events family and its capabilities use automated tools to identify incidents and events and assist in responding to them. In addition to automated tools, the identification and response to incidents and events requires planning which is typically documented in incident response and contingency plans,

and testing/reporting. The primary objective of the Manage Events family is to identify and respond to incidents and events while continuing to perform the business functions of the organization.

5.2.6.1 Prepare for and Detect Incidents and Contingencies

Purpose - Provide the ability to automate the process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected events from becoming incidents, and responding to incidents and contingencies when necessary. Review events selected for monitoring and update, as appropriate.

NIST SP 800-53 Controls - Controls related to the process of generating, transmitting, storing, analyzing, and preparing for the response to events and incidents are AU-2, AU-6, AU-6(4), IR-5, IR-8, and SI-4. Controls related to the process of preparing for contingencies are CP-2 and CP-4.

Targets Attack Vectors - Lack of effective security logging and analysis may allow attackers to hide their location, and activities on compromised machines. Without audit logs, an attack may go unnoticed indefinitely. Ineffective contingency plans may allow unforeseen events to cause a system/network to be unavailable or degraded to such an extent the organization cannot perform its business functions.

Implementation Approach - Deploy a logging platform as a management tool for log aggregation and consolidation from multiple sources to enable analysis of correlated events and logs. Develop effective contingency plans allowing systems/networks to effectively operate under emergencies and disasters. Review events selected for monitoring annually and revise, as appropriate.

GSA Enterprise Tool(s) - GSA uses an Enterprise Logging Platform (ELP) tool to centralize review and analysis of audit records from multiple systems to identify correlated events. The ELP tool detects and alerts designated personnel on anomalous events. Incident Response and Handling Tools used by GSA are detailed in Appendix C of CIO-IT Security-01-02, *"Incident Response."*

5.2.6.2 Respond to Incidents and Contingencies

Purpose - Provide the ability to use automation to assist in the process of responding to events occurring in an information system or network or events impacting them, analyzing the events/incidents and taking appropriate action to eliminate or mitigate the threats while allowing the business functions of the organization to continue. Reporting events/incidents, as necessary, to the appropriate parties/organizations. Executing contingency plans when emergencies or disasters require them to be implemented.

NIST SP 800-53 Controls - Controls related to the process of responding to events and incidents are IR-5, IR-6, IR-8, and SI-4. Controls related to responding to contingencies are CP-2 and CP-4.

Targets Attack Vectors - Lack of effectively responding to events or incidents identified by security logging and analysis may allow attackers to continue to perform malicious activities against the system/network and organization. Without effective response, an attack may last longer and subject the organization to extended malicious actions. Ineffective contingency plans may allow systems/networks to be adversely affected to a degree that the organization cannot fulfill its business functions.

Implementation Approach - Deploy Intrusion Detection Systems/Intrusion Preventions Systems (ISDs/IPSS) along with an ELP tool to identify events and incidents that require action. Develop an Incident Response Plan, train and test it to ensure response is timely and effective. Incident Response and Handling Tools used by GSA are detailed in Appendix C of CIO-IT Security-01-02. Develop a Contingency Plan, train and test it to ensure reaction and recovery is timely and effective.

GSA Enterprise Tool(s) - GSA uses IDSs/IPSS and an ELP tool to centralize review and analysis of event and incident data from multiple systems to correlate events and incidents. These tools detect and alert designated personnel when anomalous events/incidents occur so they can take action as required by the Incident Response Plan. The [GSA Enterprise Continuous Monitoring Tools](#) Google Sheet provides a detailed list of tools used to respond to events and incidents.

Appendix A – ISCM Controls

Table A-1 provides, for information systems accepted into the OA Program, common control responses for CA-2, CA-7, and CA-8(7) or standard control responses that require updating within a system’s SSP. Table A-2 identifies GSA’s automated ISCM controls along with a brief implementation description. Table A-3 identifies GSA’s process based ISCM controls along with a brief implementation description.

Table A-1: OA Program Common Control Responses

CA-2, Security Assessments	Control Summary Information
Implementation Status	Implemented
Control Origination	Hybrid Control (Shared Between the [ACRONYM] and GSA OCISO CIO-IT Security-12-66.
Part a	<p><u>GSA OCISO (Common Control):</u> GSA’s OCISO A&A security assessment processes are documented within CIO-IT Security-06-30, “Managing Enterprise Risk.” GSA security assessment plans are created per each system’s A&A requirements. Each plan describes the scope of the system’s assessment to include the security controls under assessment, the assessment procedures used to determine the security controls effectiveness, the assessment environment, identification of the assessment team, and the assessment team’s roles and responsibilities. GSA OCISO has established an Information System Continuous Monitoring (ISCM) Ongoing Authorization (OA) Program and is defined by CIO-IT Security-12-66, “Information Security Continuous Monitoring Strategy & OA Program.” OA Information systems are required to have completed a GSA A&A within 18 months prior to their acceptance into the OA Program and issuance of their OATO letter. Upon acceptance into the OA Program, systems undergo Biannual Performance Metric Reviews (PMRs) as defined by CIO-IT Security-12-66. The OA Program’s PMRs function as periodic system security control assessments, per the OA Program’s requirements.</p> <p><u>[ACRONYM](System-Specific Controls):</u> [ACRONYM] has been accepted into GSA OA Program and currently operates with an OATO.</p>
Part b	<p><u>GSA OCISO(Common Control):</u> GSA OCISO has established an OA Program and is defined by CIO-IT Security-12-66. For detailed annual ISCM Program assessment requirements, please reference CIO-IT Security-12-66.</p> <p><u>[ACRONYM] (System-Specific Controls):</u> [ACRONYM] has been accepted into GSA’s OA Program and currently operates with an OATO. As a requirement of maintaining the system’s OATO, the designated [ACRONYM] OA ISSO is required to annually assess the security controls of the information system and complete the annual FISMA Self-Assessment. Upon completion of the annual control assessment, the OA ISSO requests the review and SSP signature approvals from the system’s assigned OA ISSM and System Owner.</p> <p>[date] last [ACRONYM] SSP review was completed</p>

CA-2, Security Assessments	Control Summary Information
Part c	<p><u>GSA OCISO(Common Control):</u> GSA’s OCISO A&A security assessment processes are documented within CIO-IT Security-06-30. As an output of an A&A, the OCISO produces a Security Assessment Report (SAR). GSA OCISO has established an OA Program and is defined CIO-IT Security-12-66. As part of the OA Program system onboarding activities, an OA Onboarding Assessment Report (OAR) is created and documents the results of the system’s OA Program assessment. Results of the OA Program’s Biannual Performance Metric Reviews (PMRs) are documented and disseminated using internal email communications. Please reference CIO-IT Security-12-66 for more details.</p> <p><u>[ACRONYM] (System-Specific Controls):</u> [ACRONYM] has been accepted into GSA’s OA Program and currently operates with an AO ATO. As a requirement of maintaining the system’s AO ATO, the designated [ACRONYM] OA ISSO is required complete GSA’s Annual FISMA Self-Assessment for the information system. The results of the system’s FY FISMA Self-Assessment, reports upon the results of the assessment activities performed by the OA ISSO.</p>
Part d	<p><u>GSA OCISO(Common Control):</u> As an output of [ACRONYM] last A&A the OCSIO issued a Security Assessment Report (SAR). The SAR was disseminated to the system’s OA ISSO, OA ISSM, System Owner, and AO. The OA Program’s Onboarding Assessment Report (OAR) and Biannual Performance Metric Review (PMR) results are disseminated to the system’s OA ISSO, OA ISSM, System Owner, CISO, and AO. Please reference CIO-IT Security-12-66 for more details.</p> <p><u>[ACRONYM] (System-Specific Controls):</u> The [ACRONYM] OA ISSO is required to maintain the system’s last OCISO A&A SAR within its Archer GRC A&A documentation repository.</p>

CA-7, Continuous Monitoring	Control Summary Information
Implementation Status	Implemented
Control Origination	Hybrid Control (Shared Between the [ACRONYM] and GSA OCISO CIO-IT Security-12-66.
Part a	<p><u>GSA OCISO(Common Controls):</u> GSA OCISO has established an OA Program and is defined by CIO-IT Security-12-66. For detailed ISCM Program system specific monitoring metric requirements, please reference CIO-IT Security-12-66.</p>
Part b	<p><u>GSA OCISO(Common Controls):</u> GSA OCISO has established an OA Program and is defined by CIO-IT Security-12-66. For detailed OA Program system specific monthly and annual monitoring requirements, please reference CIO-IT Security-12-66.</p>

CA-7, Continuous Monitoring	Control Summary Information
Part c	<p><u>GSA OCISO(Common Controls):</u> Systems accepted into the OA Program are required to annually complete their assigned GSA FISMA Self-Assessments and complete an OA Critical Control Walk-Through. For detailed OA Program Control Assessment requirements, please reference CIO-IT Security-12-66.</p> <p><u>[ACRONYM] (System-Specific Controls):</u> Information systems accepted into the OA Program are required to assess their security controls annually. The designated [ACRONYM] OA ISSO either performs or facilitates the defined ISCM Program assessment requirements.</p>
Part d	<p><u>GSA OCISO(Common Controls):</u> Biannually the OA Program Manager/ISP performs a system specific FY Q2 & Q4 Performance Metric review of each information system, based on the OA Program’s defined metrics. For detailed OA Program metric requirements, please reference CIO-IT Security-12-66.</p> <p><u>[ACRONYM] (System-Specific Controls):</u> The designated [ACRONYM] OA ISSO is required to support the system specific OA Program Performance Metric reviews as scheduled. Additionally the OA ISSO is responsible for ongoing monitoring of their assigned system’s OS Program metric requirements. Monitoring is performed either via automated or non-automated monitoring activities.</p>
Part e	<p><u>GSA OCISO(Common Controls):</u> OA Program performs correlation and analysis of all security related information identified by the program’s assessments and monitoring activities. Communication is performed by OA Team/ISP to the system’s assigned OA ISSO, System Owner, and AO biannually or as required by event driven activities.</p>
Part f	<p><u>GSA OCISO(Common Controls):</u> Response actions, based upon OA Program assessments or monitoring activities. Are communicated by OA Team/ISP to the system’s assigned OA ISSO, System Owner, and AO.</p> <p><u>[ACRONYM] (System-Specific Controls):</u> The designated [ACRONYM] OA ISSO is required track all OA Program response actions identified within the system’s POA&M and/or via an Acceptance of Risk (AOR) when applicable.</p>
Part g	<p><u>GSA OCISO(Common Controls):</u> Biannually the OA Program Manager/ISP reports the results of the FY Q2 & Q4 Performance Metric reviews, to each information system’s System Owner and AO.</p> <p><u>[ACRONYM] (System-Specific Controls):</u> The designated [ACRONYM] OA ISSO is responsible for providing stakeholder system specific security status reports, based upon the system’s security management requirements. Stakeholders included in such reporting may include, but are not limited to; OA ISSM, System Owner, AO, CO/COR, Program Managers, System Project Managers, and custodians. OA ISSO monthly system security status reporting is performed via Archer GRC assigned system ISSO Checklist.</p>

CM-8(7), Information System Component Inventory Centralized Repository	Control Summary Information
Implementation Status	Implemented
Control Origination	Shared Between the [ACRONYM] and GSA EIO
<p>NIST Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. Centralized repositories of information system component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner).</p>	
<p>**Instructions: GSA EIO Common Control response to be used by information systems which their full inventory is managed using BigFix.</p> <p><u>GSA EIO(Common Control):</u> Control requirements are implemented for [ACRONYM] as an inherited control, per GSA EIO center OS management of BigFix agent deployments on the GSA network.</p> <p><u>[ACRONYM](System-Specific Controls):</u> The designated [ACRONYM] OA ISSO is responsible for ensuring the system’s inventory is up-to-date and all BigFix agents have been deployed to the identified system’s OS. Monthly inventory change reporting and OA ISSO reviews ensures the [ACRONYM] BigFix reporting is continuously up-to-date.</p>	

Table A-2: Automated ISCM Controls

Control	Control Name	Implementation Information
AU-2	Audit Events	Systems are to comply with the GSA hardening guides applicable to components in their inventory, including the events required to be audited by the associated security benchmarks. Systems' configurations are to be verified using GSA's CDM tools.
AU-6	Audit Review, Analysis, and Reporting	Audit records are to be integrated with the Enterprise Logging Platform. This integration automates much of the process of analyzing logs for inappropriate or unusual activity.
CM-2	Baseline Configuration	System's baseline compliance is to be verified using GSA's CDM tools.
CM-2(1)	Baseline Configuration Reviews and Updates	System's baseline updates are to be verified using GSA's CDM tools.
CM-2(2)	Baseline Configuration Automation Support for Accuracy / Currency	System baseline configuration information is to be maintained using GSA's CDM tools.
CM-6	Configuration Settings	All systems must adhere to GSA hardening guides, United States Government Configuration Baseline, NIST guidelines, Center for Internet Security (CIS) Benchmarks (Level 1), or industry best practice guidelines, as deemed appropriate by the AO. All information systems must use the Security Deviation Request Form to document and get approval for any deviations from GSA agency-wide hardening guides.
CM-6 (1)	Configuration Settings Automated Central Management / Application / Verification	System's baseline updates are to be verified using GSA's CDM tools.
CM-7	Least Functionality	System's compliance with the hardening guides, including only having essential functions, ports, protocols, and services enabled are to be verified using GSA's CDM tools.
CM-7 (4)	Least Functionality Authorized Software / Blacklisting	Systems are to have GSA's enterprise security tools deployed to identify software by a digital fingerprint and deny software on the blacklist from executing.
CM-7(5)	Least Functionality Authorized Software / Whitelisting	Systems are to have GSA's enterprise security tools deployed to identify software by a digital fingerprint and allow authorized software to run, blocking everything else.
CM-8	Information System Component Inventory	Systems are to have GSA's automated tools deployed to maintain an up-to-date and readily available hardware asset inventory.
CM-8 (1)	Information System Component Inventory Updates During Installations/ Removals	Systems are to have GSA's automated tools deployed to maintain an up-to-date and readily available hardware asset inventory.

Control	Control Name	Implementation Information
CM-8 (2)	Information System Component Inventory Automated Maintenance	Systems are to have GSA's automated tools deployed to maintain an up-to-date and readily available hardware asset inventory.
CM-8 (3)	Information System Component Inventory Automated Unauthorized Component Detection	Systems are to have GSA's automated tools deployed to maintain an up-to-date and readily available hardware asset inventory.
CM-8 (4)	Information System Component Inventory Accountability Information	Systems are to have GSA's automated tools deployed to maintain an up-to-date and readily available hardware asset inventory.
CM-8(5)	Information System Component Inventory No Duplicate Accounting of Components	Systems are to have GSA's automated tools deployed to ensure components are not duplicated in system hardware asset inventories.
CM-8(7)	Information System Component Inventory Centralized Repository	Systems are to have GSA's automated tools deployed to establish a centralized repository for hardware asset inventory.
RA-5	Vulnerability Scanning	Systems are to have GSA's automated tools deployed to identify vulnerabilities for assets (i.e., Tenable agent). Any asset that cannot have an agent installed will need to be scanned for vulnerabilities using the enterprise scan tool.
RA-5 (1)	Vulnerability Scanning Update Tool Capability	Systems need to ensure vulnerability scanning agents and tests are able to be updated on system assets.
SI-2	Flaw Remediation	Systems are to have GSA's automated tools deployed to identify flaws/required updates and remediate flaws/apply updates in accordance with GSA established timelines.
SI-2(2)	Flaw Remediation Automated Flaw Remediation Status	Systems are to have GSA's automated tools deployed to identify the status of flaws/required updates in accordance with GSA established frequencies in the 06-30-Scanning Parameter Spreadsheet or CDM tool configurations.
SI-2(3)	Flaw Remediation Time to Remediate Flaws/ Benchmarks for Corrective Actions	Systems are to have GSA's automated tools deployed to identify the time to remediate of flaws/required updates in accordance with GSA established frequencies in the CIO-IT Security-06-30 , "Managing Enterprise Risk", GSA's enterprise architecture process for managing approved updates, and the system's Configuration Management Plan.
SI-3	Malicious Code Protection	Systems are to have GSA's automated tools deployed to protect systems from malware.
SI-3(1)	Malicious Code Protection Central Management	Systems are to have GSA's centrally managed automated tools deployed to protect systems from malware.

Control	Control Name	Implementation Information
SI-4	Information System Monitoring	Systems are to deploy GSA's automated capabilities such as ELP, IDS, IPS and others to perform information system monitoring and log management and event analysis. Tools are to be capable of integrating feeds with the enterprise ELP tool OCISO uses which correlates data from many sources to support near real-time analysis of events.
SI-7	Software, Firmware, and Information Integrity	Systems are to have GSA's centrally managed automated tools (e.g., Bit9, Tripwire) deployed that detect unauthorized changes and perform integrity verification of systems.

Table A-3: Process-based ISCM Controls

Control	Control Name	Implementation Information
AC-2	Account Management	Systems are to perform an annual review and recertification of user accounts to verify if the account holder requires continued access to the system. The results of the annual user recertification process needs to be provided as part of the ISCM program annual deliverables; this document should also address AC-6 and AC-6(2).
CA-2	Security Assessments	An annual FISMA self-assessment will be performed based on controls selected by the OCISO. The specific controls, assessment test cases, and deadlines will be coordinated through Information System Security Managers (ISSMs) and Information System Security Officers (ISSOs).
CA-5	Plan of Action and Milestones	System POA&Ms must be updated at least quarterly and made available for OCISO review IAW CIO-IT Security-09-44, "Plan of Action and Milestones (POA&M)."
CA-7	Continuous Monitoring	Perform continuous monitoring activities in accordance with the ISCM Program to include reviewing GSA-defined performance metrics, remediating security vulnerabilities and reporting on the security status of the information system assets.
CA-8	Penetration Testing	All Internet facing and FIPS 199 High systems must have penetration tests performed annually and provided to OCISO IAW CIO-IT Security-11-51, "Conducting Penetration Test Exercises."
CM-9	Configuration Management Plan	System Configuration Management Plans must be reviewed annually and updated as necessary IAW CIO-IT Security-01-05, "Configuration Management."
CP-2	Contingency Plan	System Contingency Plans must be reviewed annually and updated when necessary IAW CIO-IT Security-06-29, "Contingency Planning."
CP-4	Contingency Plan Testing	System Contingency Plans must be tested annually IAW CIO-IT Security-06-29, "Contingency Planning."
IR-8	Incident Response Plan	Incident Response Plans must be reviewed annually and updated when necessary IAW CIO-IT Security-01-02, "Incident Response" and GSA's "Information Security Program Plan."
PL-2	System Security Plan	System Security Plans must be reviewed annually and updated when necessary IAW CIO-IT Security-06-30, "Managing Enterprise Risk." ISSOs are required to perform annual SSP reviews and sign offs. System Owner, ISSM and ISSOs should all be signatories.
AR-2	Privacy Impact and Risk Assessment	PTAs/PIAs must be reviewed annually and updated when necessary IAW the ISPP and GSA Privacy Program requirements.

Appendix B – References

The following Federal Laws, Regulations, Guidance, and Standards, and GSA Directives and Guides provide additional information on security, ISCM, and OA.

Note: GSA updates its IT security policies and procedural guides on independent biennial cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws and Regulations:

- [FISMA 2014](#), Public Law 113-283, “Federal Information Security Modernization Act of 2014”
- [Executive Order 13800](#), “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”
- [OMB Circular A-130](#), “Managing Information as a Strategic Resource”
- [OMB Memorandum M-14-03](#), “Enhancing the Security of Federal Information and Information Systems”

Federal Guidance and Standards:

- [Federal Information Processing Standard \(FIPS\) 199](#), “Standards for Security Categorization of Federal Information and Information Systems”
- [NIST SP 800-37, Revision 2](#), “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy”
- [NIST SP 800-53, Revision 4](#), “Security and Privacy Controls for Federal Information Systems and Organizations”
- [NIST SP 800-137](#), “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”
- [NISTIR 8011, Volume 1](#), “Automation Support for Security Control Assessments: Overview”
- [NISTIR 8011, Volume 2](#), “Automation Support for Security Control Assessments: Hardware Asset Management”
- [Cybersecurity Framework](#), “Framework for Improving Critical Infrastructure Cybersecurity”

GSA Directives and Guides:

- [GSA Order CIO 2100.1](#), “GSA Information Technology (IT) Security Policy”
- [GSA Order CIO 2101.2](#), “GSA Enterprise Information Technology Management (ITM) Policy”
- [GSA Order CIO P 2181.1](#), “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook”
- [GSA Order ADM P 9732.1E](#), “Personnel Security and Suitability Program Handbook”

The guidance documents below are available on the GSA IT Security [Procedural Guides InSite](#) page.

- CIO-IT Security 01-02, “Incident Response”
- CIO-IT Security 01-05, “Configuration Management”

- CIO-IT Security-01-08, *“Audit and Accountability”*
- CIO-IT Security 06-29, *“Contingency Planning”*
- CIO-IT Security-06-30, *“Managing Enterprise Risk”*
- CIO-IT Security-09-44, *“Plan of Action and Milestones (POA&M)”*
- CIO-IT Security 17-80, *“Vulnerability Management Process”*
- CIO-IT Security-18-90, *“Information Security Program Plan”*