IT Security Procedural Guide: Vulnerability Management Process CIO-IT Security-17-80

Revision 3

May 19, 2022

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Version – February 6, 2017		
1	Nussdorfer / Wilson / Klemens	Created vulnerability management procedural guide to document how GSA identifies vulnerabilities and reports on them for resolution	Updated to reflect and implement most current NIST SP 800-53 Rev 4 and GSA requirements.	All
		Revision 1 – August 21, 2019		
1	Nussdorfer	Replaced references to HP WebInspect with Netsparker and added references to Nessus Agents	To reflect the shift to a new web application scanning tool and the usage of Nessus Agents in vulnerability identification	Various
2	Heffron	Added references to Twistlock	To reflect the usage of Twistlock in Cloud vulnerability identification	Various
3	Feliksa / Dean / Klemens	Changes made throughout the document to align with current OMB, NIST, and GSA policies	Updated to align with the current version of GSA CIO 2100.1 format to latest guide structure and style, revise guidance to current GSA policies and processes	Throughout
4	Thomsen	Expanded information regarding Compliance checks using CDM tools.	CDM tools being used for compliance checks.	Section 9 and Appendices
		Revision 2 – December 30, 2021		
1	Quintananieves / Peters/ Klemens	Updates include: • Revised remediation timelines per BOD 22-01 and GSA guidance • Updated to ensure all GSA systems are in scope. • Updated tools used and descriptions of their use.	Updated to align with BOD 22-01, GSA CIO 2100.1, and current GSA tools and processes.	Throughout
		Revision 3 - May 19, 2022		
1	Quintananieves / Peters/ Klemens	Revisions included: • Updated to include CISA KEV remediation verification and AOR sections. • Added information on C-CAR requirements.	Updated to reflect current processes and guidance.	Throughout

Approval

IT Security Procedural Guide: Vulnerability Management Process, CIO-IT Security 17-80, Revision 3, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

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

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Policy 1
1.4 References 3
2 Roles and Responsibilities 3
2.1 Authorizing Official (AO) 3
2.2 Information Systems Security Manager (ISSM) 4
2.3 Information Systems Security Officer (ISSO) 4
2.4 System Owners 4
2.5 Custodians 5
2.6 System/Network Administrators 5
2.7 GSA SecOps Scanning Team Members 5
3 GSA General Vulnerability Management Procedures 5
3.1 Implementation of NIST Controls 5
3.2 Adherence to Federal Laws, Regulations, Directives, and Guidance 7
3.2.1 DHS CISA Cybersecurity Directives 7
3.2.2 BOD 18-01 – Enhance Email and Web Security 8
3.2.3 BOD 19-02 – DHS Cyber Hygiene Scanning Program 8
3.2.4 BOD 20-01 – Develop and Publish a Vulnerability Disclosure Policy 8
3.2.5 BOD 22-01 – Reducing the Significant Risk of Known Exploited Vulnerabilities 8
4 Vulnerability Management 9
4.1 GSA Scanning Capabilities 9
4.2 Vulnerability Scanning Process 9
4.2.1 Inventory Updates by ISSOs 9
4.2.2 Scanning Tool Updates 10
4.2.4 Scan Issue Mitigation 12
4.3 Vulnerability Scan Reports 12
4.3.1 General Reports 12
4.3.2 Executive Reports 13
4.3.3 Ad Hoc Reports 13
4.3.4 Documenting Report Reviews 13
4.4 Vulnerability Tracking and Remediation Verification 13
4.4.1 Vulnerability Tracking 13
4.4.1 CISA KEV Remediation Enforcement 14
4.4.2 CISA KEV AORs 14
4.5 Re-Classification/Recasting of Known Vulnerabilities 14
4.6 False-Positive Handling 15
5 Configuration Settings Management (CSM) 15
5.1 CSM Scanning 15
5.2 CSM Reporting 16
5.2.1 BigFix Compliance Portal 16
5.3 CSM Deviations 16
5.4 CSM Accounting, Compliance and Reporting 17
5.4.1 CSM Accounting 17
5.4.2 CSM Compliance Reporting 17

Appendix A – Risk Level Identification 18
Appendix B – GSA Deadlines to Remediate Vulnerabilities 19
Appendix C – ISSO Vulnerability Management Tasks 20
Appendix D – BigFix Report Recommendations 21
Appendix E – Example of CSM Performance Management 22

List of Tables

Table 4-1: GSA Vulnerability Scanning Capabilities 9
Table 4-2: Scanning Schedule 10
Table 5-1: Scanning Tool Applicability 16
Table 5-2: BigFix Reports 16
Table 5-3: Configuration Setting Compliance Timeline 17
Table A-1: Risk Level Identification Table 18
Table B-1: Corrective Action Timelines 19
Table C-1: ISSO Vulnerability Management Tasks Table 20
Table D-1: Custom CSM Reporting Fields 21
Table E-1: Non-Compliant System 22
Table E-2: Compliant System 22

Notes:

- Hyperlinks in running text 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 web page or document listed in Section 1.4.
- 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

The General Services Administration (GSA) Chief Information Security Officer (CISO) is responsible for implementing and administering an information security program to protect the agency's information resources, support business processes and the GSA mission. One part of the program is the establishment of a vulnerability management process, this guide describes that process. This guide addresses the identification of vulnerabilities affecting GSA systems using various security tools and communicating the tool results to appropriate personnel for remediation, including the remediation of vulnerabilities that are published as part of the Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency's (CISA) Cybersecurity Directives, including the Known Exploitable Vulnerability (KEV) Catalog, or announced per the Federal Cybersecurity Coordination, Assessment, and Response (C-CAR) protocol.

1.1 Purpose

The purpose of this guide is to describe the procedures the GSA CISO has established to identify and address vulnerabilities affecting GSA's systems.

1.2 Scope

This guide must be followed by all GSA Federal employees and contractors managing (i.e., finding, reporting, tracking) vulnerabilities on GSA information systems and data. All GSA systems, Contractor or Federal as defined below, must adhere to the timelines described in Section 3 this guide.

- **Contractor System.** An information system in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.
- **Federal System (i.e., Agency System).** An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.

1.3 Policy

GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy" contains the following policy statements regarding requirements related to vulnerability management.

11. Contractor Operations.

> *a. GSA System Program Managers and Contracting Officers shall ensure that the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on*

behalf of GSA, including but not limited to systems operating in a Cloud Computing environment. In addition, GSA shall ensure that the contract allows GSA or its designated representative (i.e., third-party contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of the security controls. This requirement includes, but is not limited to: documentation review, server configuration review, vulnerability scanning, code review, physical data center reviews, and operational process reviews and monitoring of Service Organization Control 2 and Statements on Standards for Attestation Engagements (SSAE) 18 reports.

b. The security controls implemented as part of contracts and task orders must include specific language that requires solutions to align with existing information security architecture. Security deliverables must be provided in a timely manner for review and acceptance by GSA. Additional information may be found in GSA CIO-IT Security-09-48, Security and Privacy Requirements for IT Acquisition Efforts and, for external information systems, in GSA CIO-IT Security-19-101, External Information System Monitoring. Note: As indicated in Chapter 1, Section 5, GSA has a deviation request process by which a deviation from approved security architecture/standards may be requested.

Chapter 3, Policy for Identify Function, states:

4. Risk Assessment.

a. Independent vulnerability testing including penetration testing and system or port scanning conducted by a third-party such as the GAO and other external organizations must be specifically authorized by the AO and supervised by the ISSM.

Chapter 5, Policy for Detect Function, states:

2. Security Continuous Monitoring.

t. Systems will be scanned for vulnerabilities of operating systems and web applications periodically IAW GSA CIO-IT Security-17-80. Vulnerabilities identified must be remediated IAW GSA CIO-IT Security-06-30.

Chapter 6, Policy for Respond Function, states:

3. Analysis.

f. The OCISO will establish a vulnerability management process for identifying vulnerabilities via internal testing/scanning.

g. The OCISO will notify personnel with security responsibilities of vulnerabilities disclosed via SAAs or other external sources.

4. Mitigation.

c. IAW GSA CIO-IT Security-06-30, system vulnerabilities must be:

(1) Remediated or mitigated IAW specified timeframes;

(2) Included in a Plan of Action and Milestones; or
(3) Included in an Acceptance of Risk Letter.

1.4 References

Federal Laws, Standards, Regulations, and Publications:

- CISA Cybersecurity Directives - Listing of Emergency and Binding Operational Directives
- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- Public Law 113-283, "Federal Information Security Modernization Act (FISMA) of 2014"
- National Vulnerability Database Vulnerability Metrics, Webpage on Vulnerability Metrics
- NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment"
- NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"
- NIST CSF, "Framework for Improving Critical Infrastructure Cybersecurity"
- 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 5, "Security and Privacy Controls for Information Systems and Organizations"

GSA Policies, Procedures, Guidance:

The GSA policy listed below is available on the GSA.gov Directives Library page.

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page.

- CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk"
- CIO-IT Security-09-44, "Plan of Action & Milestones (POA&M)"
- CIO-IT Security-09-48, "Security and Privacy Requirements for IT Acquisition Efforts"
- CIO IT Security-19-101, "External Information System Monitoring"

2 Roles and Responsibilities

The roles and vulnerability management responsibilities provided in this section have been extracted and summarized from CIO 2100.1, Federal guidance, or GSA Security Operations (SecOps) Scanning Team standard operating procedures/processes.

2.1 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring vulnerability scans are able to be performed on systems and applications under their purview;

- Coordinating with the CISO and experts within the OCISO regarding the consistent management of cybersecurity risks across GSA.

2.2 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Coordinating the performance of vulnerability scans with ISSOs and the SecOps Scanning Team;
- Reviewing ISSO checklists submitted in Archer GRC to ensure vulnerability management adheres to GSA policies and requirements and coordinating with ISSOs, as necessary, for systems under their purview.

2.3 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Coordinating the performance of vulnerability scans (scheduled and ad hoc) with System Owners, ISSMs, and the SecOps Scanning Team;
- Working with the System Owner and ISSM to develop, implement, and manage POA&Ms regarding identified vulnerabilities for their respective systems IAW GSA CIO-IT Security-09-44;
- Evaluating known vulnerabilities (e.g., vulnerability summaries provided by ISE and scan reports provided by the SecOps Scanning Team) with system personnel for remediation within defined response times and to ascertain if additional safeguards are needed;
- Verifying all assets (hardware and software) in the A&A boundary (and only those assets) for systems they are the assigned ISSO are scanned in accordance with GSA policies and procedures (i.e., maintain an accurate inventory);
- Working with the SecOps Scan Team to resolve scanning issues (e.g., authentication issues, unreachable hosts).

Note: Appendix C specifies at a more granular level ISSO tasks and associated deadlines applicable to the vulnerability management process.

2.4 System Owners

Responsibilities include the following:

- Coordinating the performance of vulnerability scans with ISSMs, ISSOs, and the SecOps Scanning Team;
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms regarding scanning results for their respective systems in accordance with CIO-IT Security-09-44;
- Coordinating with the ISSO to ensure all assets (hardware and software) in the A&A boundary (and only those assets) for systems under their purview are scanned in

accordance with GSA policies and procedures;
- Identifying, scheduling, and ensuring the completion of actions to remediate vulnerability and configuration/compliance scan findings (e.g., security hardening, configuration changes, software patches) within defined response times.

2.5 Custodians

Responsibilities include the following:

- Coordinating the running of vulnerability scans (e.g., identifying false positives) with System Owners and the SecOps Scanning Team;
- Coordinating with System Owners, ISSMs, and ISSOs to ensure vulnerability and configuration/compliance scans can be accomplished, cover all assets, and actions are taken to address findings.

2.6 System/Network Administrators

Responsibilities include the following:

- Implementing the appropriate security requirements consistent with GSA IT security policies and hardening guidelines;
- Coordinating the performance of vulnerability scans with System Owners, ISSOs, and the SecOps Scanning Team;
- Applying patches/updates, configuration changes, and other remediation efforts to address vulnerabilities, as appropriate, within required timeframes.

2.7 GSA SecOps Scanning Team Members

Responsibilities include the following:

- Updating vulnerability scanning tools and configuring them in accordance with GSA requirements.
- Scheduling and conducting vulnerability scans and troubleshooting any issues.
- Producing, reviewing, and distributing vulnerability scanning reports.

3 GSA General Vulnerability Management Procedures

All GSA systems must adhere to the following general requirements regarding vulnerability management. Appendix B, Table B-1, Corrective Action Timelines, provides information on remediation timelines for BODs and GSA's standard vulnerability management process.

3.1 Implementation of NIST Controls

GSA systems must implement NIST controls RA-5, Vulnerability Monitoring and Scanning, and SI-2(3), Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions in accordance with the frequencies and timelines established in the control statements and

parameters as indicated below (only the parts of RA-5 and SI-2(3) that address frequencies or timelines are listed).

RA-5:

a. Monitor and scan for vulnerabilities in the system and hosted applications [*weekly authenticated scans for operating systems (OS)-including databases, monthly unauthenticated scans for web application, annual authenticated scans for web applications*] and when new vulnerabilities potentially affecting the system are identified and reported;
d. Remediate legitimate vulnerabilities [
(1) BOD Timelines
(a) Within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.
(b) Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.
(c) Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
(2) GSA Standard Timelines
(a) Within 30 days for Critical (Very High) and High vulnerabilities.
(b) Within 90 days for Moderate vulnerabilities.
(c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services.]
in accordance with an organizational assessment of risk;

SI-2(3):

(b) Establish the following benchmarks for taking corrective actions: [
(1) BOD Timelines
(a) Within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.
(b) Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.
(c) Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
(2) GSA Standard Timelines
(a) Within 30 days for Critical (Very High) and High vulnerabilities.
(b) Within 90 days for Moderate vulnerabilities.
(c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services.]

As indicated in the Section 2 every role listed has some responsibility to ensure the required scanning activities can and are performed for all GSA systems, applications, and assets; and that remediation actions are taken.

3.2 Adherence to Federal Laws, Regulations, Directives, and Guidance

CIO 2100.1 establishes the controls/requirements for compliance to Federal Laws and regulations, including DHS CISA Cybersecurity Directives and NIST publications. CIO-IT-Security-06-30 reinforces these requirements and specifies requirements for vulnerability scanning and flaw remediation. CIO-IT Security-09-48 reinforces the requirements to adhere to GSA policies and requirements for all IT acquisitions (i.e., contracted systems), and CIO-IT Security-19-101, establishes the means by which GSA monitors external contractor systems for compliance with GSA's requirements.

In addition to the NIST requirements specified in the previous section, the processes defined in GSA's IT Security Policy and the procedural guides identified above, the primary adherence requirements are generated by CISA's Cybersecurity Directives which are explained in the following sections.

3.2.1 DHS CISA Cybersecurity Directives

DHS CISA develops and oversees the implementation of Binding Operational Directives (BODs), Emergency Directives (EDs), and the C-CAR protocol which require action on the part of civilian Executive Branch agencies that fall under CISA's authorities. GSA is an agency that falls under CISA's authorities. Descriptions of BOD, ED, and C-CAR are provided below.

BOD. A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

ED. Section 3553(h) of title 44 U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "*issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.*"

C-CAR. DHS serves a key role for the federal civilian executive branch in expediting the resolution of significant cybersecurity vulnerabilities. This role begins when we first learn of a new significant vulnerability. Upon doing so, either through a public announcement, our standing relationships with the cybersecurity vendor and research community, or our own activities, our first priority is to rapidly promulgate actionable information to our partners. For federal civilian agencies, our principal tools for this immediate dissemination are the C-CAR calls and alerts via standing portals. C-CAR calls allow DHS to quickly convey information to CISOs across the federal civilian government.

Although all CISA Cybersecurity Directives and C-CARs are applicable to GSA's systems, the following sections highlight specific directives that are focused on vulnerability management, identification, and remediation.

3.2.2 BOD 18-01 – Enhance Email and Web Security

This BOD focuses on Federal cyber hygiene and sets forth the requirement that all GSA web applications be compliant with the following items.

- All publicly accessible Federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS),
- SSLv2 and SSLv3 are disabled on web servers, and
- 3DES and RC4 ciphers are disabled on web servers

3.2.3 BOD 19-02 – DHS Cyber Hygiene Scanning Program

This BOD applies to all current and future critical vulnerabilities identified in the weekly "Cyber Hygiene report" issued by DHS CISA. SecOps receives this report from CISA, notifies appropriate personnel and coordinates remediation or mitigation. SecOps will perform all reporting to CISA, including population of a partially completed remediation plan sent by CISA if GSA has any overdue, in-scope vulnerabilities. If a remediation plan is received, SecOps will complete the following fields in the remediation plan in cooperation with system personnel:

1. Vulnerability remediation constraints;
2. Interim mitigation actions to overcome constraints;
3. Estimated completion date to remediate the vulnerability.

3.2.4 BOD 20-01 – Develop and Publish a Vulnerability Disclosure Policy

This BOD requires each agency to develop and publish a vulnerability disclosure policy (VDP) and maintain supporting handling procedures. It specifies a VDP as an essential element of an effective enterprise vulnerability management program and critical to the security of internet-accessible federal information systems.

All internet-accessible systems within GSA are required to be onboarded to the GSA vulnerability disclosure program and abide by the published policy.

3.2.5 BOD 22-01 – Reducing the Significant Risk of Known Exploited Vulnerabilities

This BOD creates the CISA KEV catalog and creates remediation timelines associated with all CVEs included within the catalog. SecOps will provide alerts to ISSOs related to flagged CISA KEVs within their environments. SecOps will additionally be responsible for reporting BOD 22-01 vulnerability metrics to CISA until such time as it is automated within the CDM dashboard.

4 Vulnerability Management

The following sections provide details on GSA SecOps' scanning capabilities, processes, reports, verification, and exception handling.

4.1 GSA Scanning Capabilities

Table 4-1 identifies the vulnerability scanning tools/capabilities used by GSA.

Table 4-1: GSA Vulnerability Scanning Capabilities

Tool	Capability	Description
Tenable.sc	Vulnerability Scanning Configuration Scanning	Tenable.sc (TSC) is used to identify vulnerabilities at the operating system level. Furthermore, TSC will be used for compliance checks against GSA's configuration benchmarks for assets that cannot have a BigFix agent installed. TSC scans assets on-premise and in the cloud and conducts scans over-the-network or using an agent pre-installed on the endpoint.
BigFix Compliance	Configuration Scanning	BigFix determines how compliant a workstation or server is with their applicable security benchmark. BigFix is the primary tool for this capability.
Prisma Cloud Compute	Vulnerability Scanning	Prisma Cloud Compute is the primary tool for finding vulnerabilities in Docker images and containers. It is able to find vulnerabilities in the base docker image, as well as code libraries running within that container.
Anchore	Vulnerability Scanning	Anchore is an image vulnerability scanner used in support of containerized environment build processes.
Prisma Cloud Enterprise	Configuration Scanning	Prisma Cloud Enterprise is a Software-as-a-Service (SaaS) capability managed by SecOps. The primary purpose of the tool is the detection and alerting of common misconfigurations within cloud environments.
StackRox	Vulnerability Scanning	Stackrox is a Kubernetes native vulnerability scanning and management tool. It is the primary tool in use within GSA for securing Kubernetes clusters.
Netsparker Cloud	Vulnerability Scanning Configuration Scanning	Netsparker Cloud is a scalable multi-user online web application security scanning solution with built-in workflow tools that are used to configure, organize, and report on GSA wide Netsparker scans. Netsparker Cloud utilizes deployed Netsparker agents as sensors to perform web application scans.

4.2 Vulnerability Scanning Process

This section describes key components of the vulnerability scanning process. See Appendix A for how risk levels are assigned based on the vulnerability identification tools used at GSA.

4.2.1 Inventory Updates by ISSOs

System ISSOs are required to review and update their system inventory by the 15th of each month. This includes updating all Internet Protocol (IP) addresses associated with each of their assets. ISSOs responsible for Web applications must review and update the associated Uniform

Resource Locators (URLs) as needed. Updates to all inventories will be conducted via the applicable SecOps supplied Google inventory sheets. Any changes to inventories should be reflected in the system's System Security and Privacy Plan.

Note: Failure to update system inventory data will result in inaccurate vulnerability scan reports which, in turn, will lead to inaccurate System POA&M data and reports.

4.2.2 Scanning Tool Updates

Vulnerability tools are configured to have their plugins auto updated, where possible updates will occur during non-work hours. Leveraging the Google inventory sheets, the Scanning Team will update the target lists within the vulnerability management tools, as needed. As necessary, the Scanning Team will update the scan tool configuration (i.e., add plugins to a scan profile, etc.) to maximize the vulnerabilities tested by the tool.

4.2.3 Performing Vulnerability Scans

The Scanning Team performs various types of Ad Hoc and scheduled vulnerability scanning. The following sections describe each scan type.

4.2.3.1 Scheduled Scans

Table 4-2 provides a high-level view of scanning frequency. Additional details are available within the 06-30 Scanning Parameter Spreadsheet.

Table 4-2: Scanning Schedule

Scanning Type*	Frequency
Configuration Baseline Scans	Biweekly
Agent Scans	Every 72 hours
Container Image Vulnerability Scans	Real-time
Operating System Vulnerability Scans (includes Databases where applicable)	Weekly
Web Application – Unauthenticated Scans	Monthly
Web Application – Authenticated Scans	Annually
DHS Cyber Hygiene Scanning – Unauthenticated Scans	Weekly

*Scans are authenticated unless otherwise noted, DHS uses a less intrusive scan over the Internet

4.2.3.2 Agent Scans

To support DHS Continuous Diagnostics and Mitigation (CDM) requirements, GSA has deployed Tenable Nessus Agents to servers and workstations. The Nessus Agents are controlled and managed by an associated Nessus Manager. Agent deployments eliminate issues with failed authentication on agent-deployed hosts by continuously running and polling the Nessus Manager for new scans, rather than requiring a Nessus scanner to use enterprise credentials to login. To support the 72-hour DHS scan requirement, SecOps uses an automated script that identifies the age of the last scan for each agent within GSA and schedules a new scan as

needed. Associated “agent synchronization jobs” are run withinTenable.sc to import the agent scan results, which are then included in SecOps regular vulnerability reporting.

4.2.3.3 Supplemental Active Scans

Due to the “in host” nature of the agent scans not all plugins run. To ensure that all applicable vulnerability plugins within Tenable.sc are applied to GSA hosts during vulnerability scanning additional scans are necessary. These supplemental active scans run against all GSA hosts that contain a Nessus Agent and are conducted weekly on Thursdays.

4.2.3.4 Container Image Vulnerability Scans

To support security of Docker images and containers, GSA has deployed a Prisma Cloud Compute Console to manage security and reporting requirements of vulnerability scanning. This software gathers information from deployed agents called ‘Prisma Defenders’ which are containers running on each server running the Docker engine. Prisma Defenders provide real-time monitoring for all resources used by each running container on the system. This information is sent to the Prisma Cloud Compute Defender Console where reporting and enforcement takes place.

To support vulnerability scanning of Kubernetes environments GSA SecOps has deployed the StackRox security suite that monitors Kubernetes environments on a daily basis.

4.2.3.5 Web Application Scanning

Web application scans are conducted using the Netsparker web application testing suite. SecOps maintains this tool and is responsible for scanning and reporting out of the tool. In general Web application scans fall into two categories:

- Unauthenticated Scans
- Authenticated Scans

These scans are conducted on a timeframe set forth in Table 4-2.

4.2.3.6 Performing Ad Hoc Scans

Out of cycle, or ad hoc, vulnerability scans will be performed on an as-requested basis, at the discretion of the SecOps Scanning Team. Ad hoc scans are typically requested by ISSOs or Application Developers in order to verify the remediation of a previously identified vulnerability, support firewall change requests, or determine the security impact of any major system changes. However, they may be requested by anyone with a vested interest in the security posture of a system. Requests must be approved by the ISSM. Ad hoc vulnerability scans may be requested via a ServiceNow Request using the following steps.

1. Open Service Now
2. Select “Submit Catalog Request”
3. Select “Data Enterprise Services”

4. Select “Security Scan Requests”

Note: Ad hoc scans may be performed with or without authentication depending upon the configuration and the requirements of the request.

Note: All requested firewall changes will be supported by a vulnerability scan of the associated host IPs and web applications.

4.2.4 Scan Issue Mitigation

Following vulnerability scans, the SecOps Scanning Team will coordinate with applicable ISSOs regarding any scan related issues encountered during the scan cycle. Issues may include but are not limited to:

- Failures regarding system authentication
- Failures regarding the ability to reach systems
- Failures of scans to complete

Coordination on scan failures will be accomplished via email. As necessary, the SecOps Scanning Team will work with ISSOs to determine causes and resolve identified issues; however, it is the ISSOs responsibility to ensure that all hosts within their system are being scanned and to work with the underlying system administrators to resolve any authentication issues.

4.3 Vulnerability Scan Reports

The SecOps Scanning Team will produce and distribute vulnerability scan reports used to track vulnerabilities on assets. These reports can support an ISSO’s workflow for tracking vulnerabilities thru closure (i.e., remediation). They can contain all the required fields for understanding the vulnerabilities found on an asset, and their severity. These vulnerability reports are classified as Controlled Unclassified Information and distributed on a need-to-know basis.

4.3.1 General Reports

Tenable.sc will be configured to auto-generate and distribute to applicable ISSOs/Points of Contact (POCs) vulnerability reports listing all of the vulnerabilities identified during the weekly scans. Vulnerability reports depicting vulnerabilities identified during the monthly unauthenticated Netsparker scans will be created and distributed by the SecOps Scanning Team. ISSOs will be able to review the scan results associated with their systems via access to the scanning tools. Vulnerability reports listing vulnerabilities identified during the ‘realtime’ Prisma Cloud Compute Defender monitoring will be automatically created and distributed biweekly by the SecOps Scanning Team. A Prisma Cloud Compute Distribution’ list is maintained by SecOps for distribution.

StackRox automated reporting is conducted on a daily basis. The distribution list for these reports is maintained by the SecOps team.

4.3.2 Executive Reports

On a biweekly basis, the SecOps Scanning Team will produce and distribute Executive Reports summarizing the vulnerabilities that affect GSA system components and applicable cloud hosted environments. The systems outlined within the reports will be broken out by GSA Service/Staff Office/organization responsibility and then by individual FISMA systems. The following data breakouts will be contained within the Executive Reports:

- Number of outstanding high and critical risk vulnerabilities
- Summary of active vulnerabilities broken out by FISMA system
- Summary of vulnerabilities mitigated in the past 30 days broken out by FISMA system
- Top 10 Critical Vulnerabilities Summary
- Top 10 Critical and High Risk Vulnerability Summary
- Top 10 High and Critical Vulnerabilities Over 30 Days Old
- Top 10 Hosts with High and Critical Vulnerabilities Over 30 Days Old
- Hosts that are exposed to the Internet and have Critical Risk Vulnerabilities

These reports are distributed to applicable personnel such as AO, ISSM, ISSO, and System Owners.

Note: Authorized individuals requiring additional data breakouts may contact the SecOps Scanning Team and request a different system/vulnerability categorization scheme.

Note: Only Tenable.sc vulnerability data is included in Executive Reports.

4.3.3 Ad Hoc Reports

The SecOps Scanning Team will produce a vulnerability report of an ad hoc vulnerability scanning event, upon request. These reports will be distributed to applicable personnel such as, but not limited to ISSOs, ISSMs, AOs, and System Owners.

4.3.4 Documenting Report Reviews

The review of scan reports/results is documented via ISSO Checklists in GSA's implementation of GRC Archer. ISSOs attest they have reviewed the reports/results as part of the checklists and ISSMs approve the ISSOs' reviews when they approve the checklists.

4.4 Vulnerability Tracking and Remediation Verification

GSA tracks and verifies vulnerability remediation as described in the following sections.

4.4.1 Vulnerability Tracking

In Tenable.sc, data related to the aging of vulnerabilities will be collected and tracked by the SecOps Scanning Team and provided to Executives, ISSMs, and ISSOs during the normal reporting cycles. Vulnerabilities will mature based on the date originally identified in scan results/reports. Vulnerabilities over 30 days old will be depicted within each report. The provided associated files will contain columns depicting when vulnerabilities were 'first

discovered' and 'last observed.' ISSMs and ISSOs should leverage the reports and associated files to assist with prioritizing mitigation activities.

Prisma Cloud Compute does not track 'first discovered' or 'last observed' information on vulnerabilities on a per image basis. Its reports contain links to each specific vulnerability which can be followed to find the date on which the vulnerability was announced to the open community. This date should be used to calculate the 30-day and 90-day countdown for prioritizing mitigation and resolution.

Web Application scanning conducted within Netsparker has the ability to do targeted remediation tests which can be used to mark a finding as remediated. Additionally, vulnerabilities can be marked as closed manually when manual testing is completed to show remediation.

See Appendix B for additional details regarding remediation deadlines.

4.4.1 CISA KEV Remediation Enforcement

For CISA KEV vulnerabilities that cannot be readily corrected, system owners will be given a 14-day grace period after the due date to patch or mitigate the KEV. After this period, the CIO and AO will be notified of the unmitigated risk and provided with one of the following recommendations:

- Shutdown the impacted system.
- Quarantine the impacted system.
- Allow an acceptance of risk (AOR) for not longer than 60 days.

After approval from the CIO and AO, the system owner has the responsibility to quarantine or shutdown vulnerable hosts until the system can be patched. The allowance and description of AORs is in the following section.

4.4.2 CISA KEV AORs

Due to the significant risk the KEVs pose to the federal government, AORs will only be authorized with CISO, CIO, and AO approval for no longer than 60 days from the KEV's due date. AOR requests should only be submitted based on an operational risk outweighing the security risk. No extensions will be offered for KEV associated AORs. If the System Owner is unable to address the KEVs within the AOR timeline a recommendation to quarantine or shutdown will follow.

4.5 Re-Classification/Recasting of Known Vulnerabilities

Special considerations may be made for the reporting of vulnerabilities associated with Acceptance of Risk (AOR) letters that have been approved per CIO-IT Security-06-30. ISSOs may request re-categorization of vulnerabilities included in AORs as follows:

- Web Application vulnerabilities may be considered false positives, therefore excluding them from vulnerability reports.
- Operating system vulnerabilities will be 'accepted' within Tenable.sc when SecOps is provided with a valid AOR
- Operating system vulnerabilities may be recast to 'informational' with supporting justification.
- Prisma Cloud Compute related vulnerabilities may be handled as 'ignored' within the PCC Console, allowing them to be untracked in future reports.

It is the responsibility of the individual ISSOs to track their associated AORs and present the SecOps Scanning Team with supporting documentation, as requested.

Note: Vulnerabilities with recast risk levels will appear in vulnerability scan reports with the assigned Common Vulnerability Scoring System (CVSS) score, however the Severity level will be shown as "Informational."

4.6 False-Positive Handling

A vulnerability identified as a "false positive" applies to a vulnerability reported where in fact none exists. Through the course of system personnel implementing remediation strategies to mitigate identified vulnerabilities, it may be determined that a reported vulnerability is actually a false positive. Following the verification of a false positive by technical/subject matter experts, an ISSO, in coordination with the system owner/personnel, may request the associated identified 'vulnerability' be reclassified in the same manner as described in Section 7. As with all vulnerability scanning exceptions, this request must be routed through and approved by the ISSM and SecOps Scanning Team.

Note: False Positives will be designated on an individual host-by-host basis. System wide exceptions will only be made with explicit approval from the CISO/SecOps.

5 Configuration Settings Management (CSM)

Configuration Settings Management (CSM) is the practice of managing our security baselines and configuring assets to comply with settings found in these baselines. This term was coined under the Continuous Diagnostics and Mitigation (CDM) program.

Two tools are used to monitor and report compliance with our baselines: BigFix Compliance and Tenable.sc. Each tool is considered authoritative for the results they provide and each tool covers different sets of assets.

5.1 CSM Scanning

Several factors determine what tool will be used for CSM scanning: location, type of asset, level of access to that asset. BigFix will be used whenever possible for CSM scanning. If a BigFix agent cannot/should not be installed on the asset, Tenable Nessus will be used. Both solutions require a configuration change on the asset and within the solution itself.

Table 5-1: Scanning Tool Applicability

Component Type	Location	CSM Tool Used
Workstation (GFE)	Anywhere	BigFix
Server	On-premise	BigFix
Server	Cloud	Tenable/Bigfix
Network Devices	On-premise	Tenable

5.2 CSM Reporting

ISSOs, ISSMs, and other personnel responsible for the security of a system can use a variety of different reports and dashboards within BigFix Compliance and Tenable Security Center to monitor their compliance scores. See Appendices D and E for additional information regarding CDM data for reporting and configuration settings.

5.2.1 BigFix Compliance Portal

Personnel can access the BigFix Compliance portal directly if they have been granted access. If access is needed, a generic request in ServiceNow can be submitted with a justification for access. Once granted, a user is automatically signed into the compliance portal using their Long Name Account (LNA).

This portal offers dashboards and the ability to create and email custom reports. Compliance reports can be customized then scheduled for delivery to a user's email inbox. ISSOs will be expected to access BigFix compliance for their reporting needs; SecOps will not publish or distribute reports for assets within BigFix.

Table 5-2: BigFix Reports

Report Type	When To Use	Important Tips
Computer	States an assets' compliance percentage against assigned baselines. Can be exported into Excel or viewed within BigFix Compliance. If viewed online in the portal, you can drill-down into the compliant and non-compliant settings for a particular host.	• Filter the list of assets using the "GSA FISMA System" field. • Filter on Configuration baseline to ensure calculations do not include two checklists.
Checklist	Used to determine compliance with a checklist.	• Filter the list of assets using the "GSA FISMA System" field. • Select a FISMA System. • Select Checklists.

5.3 CSM Deviations

Some configuration settings cannot be applied to an asset(s) for valid reasons. In these cases, the ISSO should request a deviation for these settings; otherwise, compliance scores will be calculated and reported incorrectly. Any deviations, exceptions, or other conditions not

following GSA policies and standards must be submitted using the Security Deviation Request Google Form. Once the deviation is documented and approved, those settings can be excluded from compliance score calculations.

5.4 CSM Accounting, Compliance and Reporting

5.4.1 CSM Accounting

A FISMA system must monitor compliance to all of the configuration settings required by GSA hardening guides. Each configuration setting must be covered by one of the following clauses:

- **The configuration setting is compliant** - The asset's setting is either:
    1. Equal to the setting required, or
    2. More restrictive than the setting required.
- **The configuration setting is not compliant** - The asset is configured with a more liberal setting than what is required. In this case, the non-compliant configuration setting needs to be accounted for in one of the following ways:
    1. Deviation - The non-compliant setting is covered by an approved deviation.
    2. Plan of Action and Milestone (POA&M) - If the composite compliance percentage of all assets with a single operating system is below 85% for over 90 days, a POA&M must be created for the non-compliant operating system.

Table 5-3: Configuration Setting Compliance Timeline

Timeline	Expectation
Day 1 – Day 90	Harden asset to 85% compliance or seek approval for required deviations.
Day 91+	Create/maintain POA&M (per operating system) if non-compliant setting percentage is below 85% (approved deviations not included in percentage calculation).

5.4.2 CSM Compliance Reporting

A FISMA systems' compliance with CSM requirements is regularly reported to executives. A FISMA system will be reported as non-compliant with CSM requirements if any **GSA Operating System** benchmark within the FISMA System is reporting under 85% compliance.

Appendix A – Risk Level Identification

Table A-1: Risk Level Identification Table

Source of Risk Rating	Risk Assessment Process
Tenable.sc • (OS, including Database scans) • Configuration/Compliance scans	Use the National Vulnerability Database (https://nvd.nist.gov/cvss.cfm) qualitative ratings, when available. Tenable Security Center uses CVSS v2.0 ratings, vulnerabilities with assigned scores will be rated as listed below. • CVSS score of 0.0-3.9 will be labeled "Low" severity. • CVSS score of 4.0-6.9 will be labeled “Moderate” severity. • CVSS score of 7.0-9.9 will be labeled “High” severity. • CVSS score of 10.0 will be labeled “Critical” severity. If the vulnerability has no CVSS score the Tenable Security Center rating will be used.
Prisma Cloud Compute (OS and code library results):	Use the National Vulnerability Database (https://nvd.nist.gov/cvss.cfm) qualitative ratings. Prisma Cloud Compute uses CVSS v3.0 ratings, vulnerabilities with assigned scores will be rated as listed below. • CVSS score of 0.1-3.9 will be labeled "Low" severity. • CVSS score of 4.0-6.9 will be labeled “Moderate” severity. • CVSS score of 7.0-8.9 will be labeled “High” severity. • CVSS score of 9.0-10.0 will be labeled “Critical” severity. If the vulnerability has no CVSS score the Prisma Cloud Compute assigned rating will be used.
Netsparker (Web application scans)	Use the Netsparker vulnerability severity rating, unless otherwise reclassified/adjusted by the GSA OCISO. Netsparker uses the following severities: • Informational • Low • Medium • High • Critical

Appendix B – GSA Deadlines to Remediate Vulnerabilities

Table B-1: Corrective Action Timelines

Corrective Action Deadline	Required Actions	Target	Primary Reference
BOD Timelines			
Within 14 days	Remediate vulnerabilities added to CISA's Known Exploited Vulnerabilities (KEV) Catalog with a CVE date post FY21.	Any GSA system with the newly identified vulnerabilities.	BOD 22-01
CISA KEV catalog date or GSA Standard timelines below, whichever is earliest.	Remediate vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.	Any GSA system with the vulnerabilities listed in the CISA KEV catalog.	BOD 22-01
Within 15 days of initial detection	Remediate **Critical (Very High)** vulnerabilities for systems or services with Internet-accessible IP addresses.	Any GSA system identified in a DHS Cyber Hygiene Report with critical vulnerabilities.	BOD 19-02/ BOD 20-01
Within 30 days of initial detection	Remediate **High** vulnerabilities for systems or services with Internet-accessible IP addresses.	Any GSA system identified in a DHS Cyber Hygiene Report with high vulnerabilities.	BOD 19-02/ BOD 20-01
Standard GSA Timelines			
Within 30 days of initial detection	Remediate **Critical (Very High)** and **High** vulnerabilities.	Any GSA system identified with critical (very high) vulnerabilities.	RA-5 control parameter
Within 90 days of initial detection	Remediate **Moderate** vulnerabilities.	Any GSA system identified with moderate vulnerabilities.	RA-5 control parameter
Within 120 days of initial detection	Remediate **Low** vulnerabilities for Internet-accessible systems or services.	Any GSA Internet-accessible Web application identified with low vulnerabilities.	RA-5 control parameter
No specific deadline unless defined by the GSA OCISO	Remediate **Low/Very Low** vulnerabilities on a case-by-case basis.	Any GSA system identified with low/very low vulnerabilities.	06-30, Section 5.7.3

Appendix C – ISSO Vulnerability Management Tasks

Table C-1: ISSO Vulnerability Management Tasks Table

Task	Deadline
Coordinate with the SecOps Scanning Team pertaining to upcoming vulnerability scans.	As needed.
Evaluate known vulnerabilities with system personnel to ascertain if additional safeguards are needed.	Upon release of new vulnerabilities (e.g., Vulnerability Summaries and Advisories provided by ISE).
Review and update system inventories.	No later than the 15th of each month.
Request out of cycle, or ad hoc, vulnerability scans, as required.	As required to verify the mitigation of a previously identified vulnerability, support firewall change requests, or determine the security impact of any major system changes.
Work with the SecOps Scanning Team to determine causes and resolve issues such as unreachable systems, or authentication issues encountered during scan cycles.	As required to overcome scan related issues confronted by SecOps.
Review all vulnerability reports and associated files and document their review.	At a minimum, monthly.
Track known vulnerabilities and their remediation statuses.	Upon identification of new vulnerabilities.
Track AORs associated with their system(s). Present the SecOps Scanning Team with supporting documentation as requested, when requesting reclassification/recasting of vulnerabilities.	Upon acceptance of new AORs, and request for reclassification/recasting of vulnerabilities.
Respond to Emergency and Binding Operational Directives as they apply to the system.	Deadline as dictated by the ED or BOD, as necessary.

Appendix D – BigFix Report Recommendations

Useful fields to include in custom CSM reports from BigFix.

Table D-1: Custom CSM Reporting Fields

Field Name	Example of Data Field
Computer	E04TCM-BFROOT
Last Seen	7 Days Ago
IP Address	127.30.32.3
GSA FISMA System	EIO
Check Count	1
Total Compliant	258
Total Excepted	4
Compliance Percentage	98%

Appendix E – Example of CSM Performance Management

Example 1 - FISMA System is reported as Non-Compliant in leadership reports

A FISMA system has 3 different operating systems within it: Windows 2016, Red Hat Enterprise Linux 6, and Windows 2012. The compliance scores are reported below. This FISMA system is considered *non-compliant because the Red Hat Enterprise Linux 7 benchmark is below 85%.*

Table E-1: Non-Compliant System

Operating System	Overall Compliance	Number of Assets
Windows 2016	90%	5
Windows 2012 R2	85%	13
Red Hat Enterprise Linux 7	83%	4

Example 2 - FISMA System is reported as Compliant in leadership reports

This FISMA system has two operating systems. This system is considered compliant because all applicable OS-level baselines are 85% or above.

Table E-2: Compliant System

Operating System	Overall Compliance	Number of Assets
Windows 2016	90%	15
Windows 2012 R2	87%	10