IT Security Procedural Guide: Risk Management Strategy (RMS) CIO-IT Security-18-91

Revision 5

August 2, 2023

Office of the Chief Information Security Officer

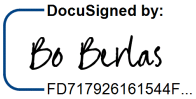
VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – March 27, 2019		
N/A	Desai	New Document		N/A
		Revision 1 – May 5, 2017		
1	Feliksa/Dean/ Klemens	Updated format and structure, align with current policies and procedures.	Reformatted document to align with current style and structure. Updated to align with current CIO 2100.1 and CIO IT Security 06-30.	Throughout
		Revision 2 – March 14, 2018		
1	Feliksa/Dean/ Klemens	Updated to integrate NIST Cybersecurity Framework and scope to IT/Cybersecurity.	Integrate NIST Cybersecurity per Executive Order 13800 and scope to information system and information security.	Throughout
		Revision 3 – June 23, 2020		
1	Dean/ Klemens	• Revised to include: • Risk Executive Function • Changed to reflect Enterprise Management Board process • Update references and roles/responsibilities • Included reference to Showstopper Controls • Updated FISMA processes description	Update to current format and style and Federal and GSA guidance.	Throughout
		Revision 4 – June 18, 2021		
1	Agosto/ Klemens/ Desai	• Revised to include: • Reorganized guide and added sections on Framing Risk, Risk Assumptions, and Risk Constraints. • Updated information on the Enterprise Management Board and subcommittees. • Included appendices for Acronyms and a Glossary. • Added information from NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM), and the Cybersecurity Risk Register	Updated to align with DHS template and current NIST and GSA guidance.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 5 – August 2, 2023		
1	McCormick/ Klemens	• Updated to reflect current GSA guidance and processes. • Edited and updated to current guide format and style. • Updated Acronym table. • Updated information on cybersecurity scoring. • Incorporated privacy risk management as part of overall risk management. • Added Chief Privacy Officer role. • Added information on CISA KEV AORs.	Updated to align with current NIST and GSA guidance.	Throughout

Approval

IT Security Procedural Guide: Risk Management Strategy (RMS), CIO-IT Security-18-91, Revision 5, is hereby approved for distribution.



Bo Berlas
GSA Chief Information Security Office

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

Table of Contents

Note: Hyperlinks in this guide are provided as follows:

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

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. The GSA program implements a mandatory set of processes and system controls based on Executive Orders (EO), Federal Laws and mandates, and National Institute of Standards and Technology (NIST) publications. The policies, procedures, and process within the program establish mechanisms and measures to establish and maintain the confidentiality, integrity, and availability of GSA systems, information, and resources. Key documents governing the GSA information security program are listed below, a more comprehensive listing of documents is provided in Appendix A.

- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- EO 14028, "Executive Order on Improving the Nation's Cybersecurity"
- Public Law 113-283, "Federal Information Security Modernization Act of 2014 (FISMA)"
- OMB Circular A-130, "Managing Information as a Strategic Resource"
- 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 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

GSA has implemented its agency-wide, risk-based information security program as defined in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy." The agency policy provides requirements to support procedures, guidelines, and formalized processes coordinated through the Office of the Chief Information Security Officer (OCISO). These elements form the foundation for GSA's information security program and define requirements for GSA systems and employees/contractors with significant security responsibilities, ensuring implementation of information security requirements.

CIO-IT Security-08-39: [Current FY] IT Security Program Management Implementation (MIP) Plan identifies the key information security activities and milestones (due dates) for managing enterprise-level risk for GSA information systems. The system specific requirements in CIO-IT Security-08-39 integrate into GSA's broader enterprise risk management approach as depicted in Figure 1-1. GSA uses a three-tiered approach for managing risk—at the organization level; mission/business process level; and the information system level.

Figure 1-1. GSA Three-Tiered Risk Management Approach

Enterprise risk at the General Services Administration (GSA) is handled by the Enterprise Management Board (EMB), chaired by the Deputy Administrator, who is also the Senior Accountable Official for Risk Management (SAORM). For cybersecurity risks, the Chief Information Security Officer (CISO), Authorizing Officials (AO), and subject matter experts facilitate the consistent application of risk management across GSA. The Enterprise Risk and Strategic Initiatives (ERSI) board identifies and monitors agency-wide risks and leads strategic initiatives to mitigate the risks and solve cross-cutting challenges. It fulfills the requirement for "an agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos.[1]"

As a collective governance body, the ERSI board is broadly responsible for establishing enterprise risk management policies, identifying enterprise level risks and risk owners, approving and monitoring mitigation strategies and controls for these risks, and providing regular briefings to the EMB. The ERSI board shall make recommendations to the EMB and identify opportunities to integrate risk with the Agency's strategy, budget planning, and resource allocation decisions. These activities ensure that significant risks to the Agency are effectively managed consistent with the Agency's risk appetite. The CISO coordinates with the CIO, a member of the EMB, to identify cybersecurity risks for consideration by the EMB. This process satisfies the ERM capability required by Office of Management and Budget (OMB) M-16-17, "OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control" and the Risk Executive (Function) identified in NIST SP 800-39.

NIST SP 800-39 describes the integration of the risk management process throughout an organization as occurring at three tiers: (1) organization level, (2) mission/business process level, and (3) information system level. The EMB addresses risk at all three tiers. At the system level, cybersecurity risks are handled by the Information System Security Officer (ISSO), Information System Security Manager (ISSM), and system owner through the assessment and authorization (A&A) process initially and then by information security continuous monitoring (ISCM). At the mission/business process level risk is managed and maintained by the AO and CISO as described in CIO-IT Security-08-39 and quarterly AO sync meetings. As depicted in

[1] NISTIR 8286, "Integrating Cybersecurity and Enterprise Risk Management (ERM)."

Figure 1-1, at the organization level the ERSI board integrates risk data from the lower levels and coordinates with the EMB as necessary to address enterprise risks.

NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations" includes security control PM-9, Risk Management Strategy, which requires an organization to develop "a comprehensive strategy to manage security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems," and "privacy risk to individuals resulting from the authorized processing of personally identifiable information." The GSA OCISO Policy and Compliance Division (ISP) has developed and maintains this document, CIO-IT Security-18-91, to establish a comprehensive approach to managing risk to the operation and use of GSA information systems. GSA follows NIST guidance when assessing and managing information systems' security and privacy risk.

The primary NIST documents and web resources guiding GSA in managing risk are:

- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments."
- 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 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View."
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."
- NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations."
- NIST Cybersecurity Framework (CSF), "Framework for Improving Critical Infrastructure Cybersecurity" and the NIST Cybersecurity Framework web page.
- NISTR 8286, "Integrating Cybersecurity and Enterprise Risk Management (ERM)."

EO 13800 requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) [i.e., the CSF] developed by NIST or any successor document to manage the agency's cybersecurity risk." GSA uses NIST SP 800-37, commonly referred to as the Risk Management Framework (RMF), as its foundation for managing risk, including the implementation of NIST SP 800-53 controls. Further information on how the CSF relates to GSA's use of the RMF, including the use of the NIST SP 800-30 risk assessment process in its overall risk management strategy, is provided in Section 10.

The listed terms are defined as follows (from the NIST online glossary) when used throughout this guide, unless otherwise stated.

- **Cybersecurity** - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
- **Cybersecurity Risk** - An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.
- **Information Security Risk** - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and

the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

- **Information System-Related Security Risks** - Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems and considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation.
- **Risk Management** - The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

1.1 Purpose

This document provides a comprehensive approach for framing, assessing, responding to, and monitoring risks associated with GSA information systems in accordance with Federal laws, regulations, and requirements and establishes GSA guidance and processes for all operating units and GSA Service and Staff Offices (SSOs) to follow.

The mission of GSA IT is to inspire and drive technology transformation by delivering innovative, collaborative, and cost-effective IT solutions and services to its customers. GSA data is an invaluable asset that requires an enterprise-wide strategy which reflects the importance of the mission and guides executive decisions about risk.

1.2 Scope

This document establishes an integrated, comprehensive approach to identify, measure, and manage risk to GSA operations, assets, and individuals associated with the operation and use of GSA information systems.

2 Governance

GSA's EMB has as one of its focus areas the management of enterprise-wide risks. The EMB and the ERSI boards use the GSA Risk Management Framework to manage risk, it consists of following main activities:

- **Identify Risk**–what is the risk, what objectives does the risk impact?
- **Assess Risk**–what is the likelihood and impact of the risk, what is the current response?
- **Analyze and Prioritize Risk**–how is the risk being addressed, what is the residual risk?
- **Manage and Escalate Risk**–Are additional responses needed, are there further actions to take, should the risk be escalated?
- **Implement and Monitor Risk**–Implement any additional response or actions needed, monitor to see if risk is being mitigated or further activities are required.
- **Communicate**–communicate with internal and external parties affected about the management of the risk and any timelines involved.

The EMB has designated the ERSI board to develop and manage ERM at GSA with the Strategy, Risk, and Performance Management Division (BIS) facilitating the board's activities. As depicted in Figure 1-1, the ERSI board works as a conduit to raise risks from the operational/system and mission/business process levels to the enterprise for consideration by the EMB, as appropriate.

2.1 Roles and Responsibilities

The complete roles and responsibilities for agency management officials and others with significant IT Security responsibilities are defined fully in Chapter 2, Security Roles and Responsibilities, of CIO 2100.1. The following sections provide extracted or paraphrased key responsibilities from CIO 2100.1 or other GSA or Federal guidance regarding managing risks associated with GSA information systems.

2.2 GSA Administrator

Responsibilities include the following:

- Developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including ensuring timely agency adoption of and compliance with security standards.
- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
- Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization.
- Ensuring that information security management processes are integrated with agency strategic and operational, and budgetary processes.
- Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the GSA Deputy Administrator on the effectiveness of the agency information security program, including the progress of remedial actions.

2.3 Risk Executive (Function)

The Risk Executive (Function) at GSA is handled by the EMB, chaired by the Deputy Administrator who is also the SAORM. For cybersecurity risks, the CISO, AOs, and subject matter experts facilitate the consistent application of risk management across GSA. As stated earlier, the EMB has engaged the ERSI board to identify and monitor agency-wide risks facing GSA, as required by OMB Circular A-123, as well as leading strategic initiatives to mitigate those risks and solve cross-cutting challenges.

Responsibilities include the following:

- Leading strategic initiatives to solve cross-cutting challenges at GSA, which may include reducing the impact of enterprise risks or capitalizing on opportunities that require a coordinated effort among SSOs.
- Identifying, vetting, and prioritizing the most significant enterprise risks to GSA’s mission, using inputs including the annual enterprise risk survey, Service and Staff Office (SSO) risk registers, and stakeholder interviews.
- In partnership with identified risk owners, developing, reviewing, and monitoring the effectiveness of mitigation strategies for major enterprise risks.
- Developing tools and frameworks for facilitating qualitative and quantitative risk assessments, monitoring the status and effectiveness of enterprise risk mitigation strategies, and conducting research on emerging risks.

2.4 Chief Information Officer (CIO)

Responsibilities include the following:

- Developing and maintaining an agency-wide GSA IT Security Program.
- Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs.
- Reporting annually, in coordination with the other senior agency officials, to the GSA Deputy Administrator on the effectiveness of the agency information security program, including progress of remedial actions.
- Participating as a member of the EMB and coordinating with other board members and the ERSI regarding cybersecurity risks in relation to overall ERM at GSA.

2.5 Chief Financial Officer (CFO)

Responsibilities include the following:

- Ensuring the sufficiency of management and information security controls pertaining to GSA's financial management systems and compliance with Federal Managers' Financial Integrity Act (FMFIA) and Federal Financial Management Improvement Act (FFMIA) requirements.
- Developing and maintaining an integrated agency accounting and financial management system, including financial reporting and internal controls, which comply with FMFIA and FFMIA requirements;
- Ensuring the appropriate security requirements of CIO 2100.1 are included in all contracts for IT systems designed, developed, implemented, and operated by a contractor that hosts GSA financial systems.
- As Performance Improvement Officer, co-chairs the ERSI, and with other board members integrates risk management into the strategic planning and decision-making processes.

2.6 Senior Agency Official for Privacy (SAOP)

Responsibilities include the following:

- Ensuring GSA information systems that contain Personally Identifiable Information (PII) address any recommendations of the SAOP as part of the system Assessment & Authorization (A&A), including addressing privacy controls in NIST SP 800-53, Revision 5–see NIST SP 800-53B , as appropriate.
- Developing, implementing, and overseeing personnel security controls for access to PII.

2.7 Chief Privacy Officer (CPO)

Responsibilities include the following:

- Participating as a member of the ERSI board and coordinating with other board members and regarding privacy risks in relation to overall ERM at GSA.
- Reporting to the GSA SAOP on the implementation and maintenance of the GSA's Privacy Program and Policies.

- Leading the Initial Agency Response Team per GSA Order CIO 9297.2C CHGE 1 in determining privacy risk during an information breach investigation.

2.8 Chief Information Security Officer (CISO)

Responsibilities include the following:

- Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies.
- Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides that are consistent with CIO 2100.1.
- Assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems supporting the operations and assets of the agency on a periodic basis.
- Testing and evaluating the effectiveness of information security policies, procedures, and practices on a periodic basis.
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
- Developing and implementing IT security performance measures to evaluate the effectiveness of technical and non-technical safeguards used to protect GSA information and information systems.
- Administering FISMA requirements and coordinating GSA’s annual FISMA security program review and Plan of Action and Milestones (POA&M) implementation.
- Concurring/non-concurring on Authorizations to Operate (ATOs) as specified in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and its related A&A procedural guides.
- As co-chair of the ERSI, along with other board members, identifying, vetting, and prioritizing enterprise risks and monitors them.
- Monitoring cybersecurity risks in the Cybersecurity Risk Register along with OCISO Directors and ISSMs/ISSOs.

2.9 Heads of Services and Staff Offices (HSSOs)

Responsibilities include the following:

- Ensuring adherence and proper implementation of GSA’s IT Security Policy.
- Ensuring the systems of record under their jurisdiction meet the requirements of the Privacy Act and GSA privacy policies and procedures.
- Ensuring that contractors performing services associated with GSA systems (such as system development, maintenance, or operation) are subject to GSA security requirements.

2.10 Authorizing Official (AO)

Responsibilities include the following:

- Identifying the level of acceptable risk for an IT system or application and determining whether an acceptable level of risk has been obtained.
- Reviewing and approving security safeguards of information systems and issuing ATO approvals for each information system and application under their purview based on the

acceptability of the implementation of security safeguards of the system (risk-management approach).
- Ensuring GSA systems are assessed via operating system and web application scans as defined in CIO-IT Security-17-80: Vulnerability Management Process. Identified vulnerabilities from the scans shall be resolved and tracked in the systems' POA&Ms in accordance with CIO-IT Security-09-44: Plan of Action and Milestones (POA&M), and CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.
- Working with the System Owners, ISSOs, and ISSMs to monitor and manage risks identified for systems under their purview in the Cybersecurity Risk Register.

2.11 Office of CISO Division Directors

Responsibilities include the following:

- Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO.
- Reviewing and approving A&A documents to be signed by the appropriate business line representatives and concurred by the CISO or appropriate OCISO personnel.
- Assisting individuals with IT Security responsibilities on security architecture and security engineering principles and practices.
- Identifying and managing cybersecurity risks in the Cybersecurity Risk Register along with ISSMs/ISSOs and the CISO.

2.12 Information System Security Manager (ISSM)

Responsibilities include the following:

- Ensuring adherence and proper implementation of GSA's IT Security Policy.
- Reviewing and coordinating reporting of Security Advisory Alerts (SAA), compliance reviews, security and privacy awareness training, incident reports, contingency plan testing, and other IT security program elements.
- Managing system assessments (including A&A package requirements and Payment Card Industry Data Security Standard (PCI DSS) Report on Compliance (for IT systems that process, store, or transmit payment card data or purchase/credit card numbers)), and forwarding them to the AO and appropriate OCISO Directors.
- Identifying and managing cybersecurity risks in the Cybersecurity Risk Register along with ISSOs, OCISO Directors, and the CISO.

2.13 Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring the system is operated, used, maintained, and disposed of in accordance with (IAW) documented security policies and procedures. Necessary security controls should be in place and operating as intended.
- Evaluating Security Advisory Alerts (SAAs) issued by the OCISO Security Operations Division and known vulnerabilities to ascertain if additional safeguards are needed and ensuring systems are patched and securely configured, as appropriate.
- Advising system owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk.

- Working with the ISSM and system owners to develop, implement, and manage POA&Ms for assigned systems in accordance with CIO-IT Security-09-44.
- Identifying and managing cybersecurity risks in the Cybersecurity Risk Register along with ISSMs, OCISO Directors, and the CISO.

2.14 System Owners

Responsibilities include the following:

- Ensuring effective implementation of GSA's IT Security Policy.
- Consulting with the ISSM and ISSO and receiving the approval of the AO and CISO, when selecting the mix of controls, technologies, and procedures that best fit the risk profile of the system.
- Participating in activities related to the A&A of the system to include security planning, risk assessments, security and incident response testing, configuration management, and contingency planning and testing.
- Ensuring that for each information system, security is planned, documented, and integrated and implemented in accordance with Federal and GSA directives, policies, and guidance.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for assigned systems in accordance with CIO-IT Security-09-44.
- Working with the ISSO and ISSM to monitor and resolve risks identified for systems under their purview in the Cybersecurity Risk Register.

2.15 Data Owners

Responsibilities include the following:

- Coordinating with system owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.
- Ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data.

2.16 Contracting Officers (COs) and Contracting Officer's Representative (CORs)

Responsibilities include the following:

- Coordinating with the CISO or other appropriate official as required, to ensure all agency contracts and procurements are compliant with the agency's information security policy and include appropriate security contracting language and security requirements in each contract.
- Ensuring new solicitations for all GSA IT systems including the security contract language from CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Effort.

2.17 Custodians

Responsibilities include the following:

- Coordinating with data owners and system owners to ensure data is properly stored, maintained, and protected.
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO.

2.18 Authorized Users of IT Resources

Responsibilities include the following:

- Complying with all GSA security policies and procedures.
- Reporting any observed or suspected security problems/incidents to the IT Service Desk.

3 GSA OCISO Divisions

The OCISO consists of the CISO and four divisions providing operational, engineering, policy, and security officer support as detailed in the following subsections.

3.1 Security Operations Division (ISO)

ISO provides real-time operational security through Security Operating Center (SOC) and enterprise network security capabilities. This division supports IT division offices by providing vulnerability scanning and operational security services at the enterprise level including managing firewalls, intrusion prevention systems, and the Enterprise Logging Platform (ELP). ISE also leads the effort to implement Zero Trust Architecture (ZTA) across the agency.

3.2 Security Engineering Division (ISE)

ISE provides security consulting and engineering support for systems and emerging IT and IT security initiatives. The division also provides incident response and technical benchmarks and manages the agency's DevSecOps program. ISE develops technical security standards and architectural security standards and provides software security testing in the support of IT systems.

3.3 Policy and Compliance Division (ISP)

ISP provides management and maintenance of the GSA POA&M, ICSM, Ongoing Authorization, and Security Awareness and Role Based Training programs. This division also manages the process to create and maintain GSA IT security policies and procedures, the coordination of cybersecurity audits, and the FISMA compliance reporting process. ISP provides information to the CISO and AOs to monitor the implementation of the GSA IT Security Policy.

3.4 ISSO Support Division (IST)

IST provides ISSO and ISSM support services to all Staff Offices and Services systems. The division facilitates integrating IT security in programs and compliance with required security and

privacy assessments. IST services assist the CISO and AOs during the assessment process to grant an Authorization to Operate (ATO).

3.5 Identity Credential, and Access Management (ICAM) Shared Service Division (ISI)

ISI supports consolidating ICAM-related capabilities to improve ICAM coordination and governance across GSA IT and development/delivery of enterprise certificate and key management capabilities. The Division is also responsible for managing Cyber Supply Chain Risk Management (C-SCRM) assurance for GSA IT and supports agencywide C-SCRM activities.

4 Risk Management Process

4.1 Framing Risk

GSA's framing of risk covers the environment in which risk-based decisions are made. It includes the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape GSA's approach to managing risk and making investment and operational decisions.

4.2 Risk Assumptions

Enterprise-level assumptions associated with the risk management strategy include:

- GSA's centralized risk management and effective governance processes allow the use of a single methodology across all mission areas.
- Key risk management personnel have appropriate training and understand and execute their roles.
- The ERM strategy provides requirements for risk assessment, response, and monitoring including cybersecurity and privacy risk.
- The five elements of NIST's CSF – Identify, Protect, Detect, Respond, and Recover – have been considered as part of GSA's cybersecurity and privacy risk management process as laid out in CIO-IT Security-06-30.
- GSA has identified High Value Assets (HVAs) supporting Primary Mission Essential Functions and Mission Essential Functions and uses this information to guide the prioritization of risk resolution.
- FIPS 199 High or Moderate systems typically have a lower risk tolerance than FIPS 199 Low systems with publicly available data. Systems with PII or other sensitive data have a lower risk tolerance than systems without such data.
- The NIST RMF is used to manage information security and privacy risk.
- Systems placed into production have undergone an authorization process based upon the RMF. Any findings from the A&A process are assessed for risk and managed via POA&Ms as described in CIO-IT Security-09-44.
- Vulnerabilities are identified through GSA's vulnerability scanning processes identified in CIO-IT Security-17-80, GSA's Vulnerability Disclosure Program, Department of Homeland Security (DHS) Cyber Hygiene reports, and other security tools.
- Potential threats are identified and documented including impact and likelihood that harm will occur.
- Appropriate processes have been developed to detect and respond to a cybersecurity incident as described in CIO-IT Security-01-02: Incident Response (IR).

- GSA utilizes lessons learned from incident response to improve response and recovery processes and reduce risk in the future.

4.3 Threat Sources

The OCISO ISO division identifies the threat landscape for GSA and assists with correlating the threat scenarios or viable threats with existing vulnerabilities that these threats can take advantage of in the GSA environment. ISO also manages GSA's Threat Awareness Program, as described in CIO-IT Security-01-02. ISO reviews indicators of compromise (e.g., domains/IP addresses of known malicious actors, hashes of malicious files, traffic excerpts of suspicious activity) from threat intelligence for actionable information and shares this information with relevant system owners, the Cybersecurity and Infrastructure Security Agency (CISA), and other government agencies as needed. CISA provides guidance through the Federal Cybersecurity Coordination, Assessment, and Response (C-CAR) protocols to coordinate and communicate threat intelligence information with GSA and other Federal agencies. CISA also develops and oversees Cybersecurity Directives (Binding Operational Directives [BODs] and Emergency Directives [Eds]) identifying threats that require action on the part of certain Federal agencies in the civilian Executive Branch. ISO implements proactive blocking of Internet Protocol (IP) addresses, Uniform Resource Locators (URLs), hashes, and fraudulent email senders, as necessary. Appendix C: Incident Response and Handling Tools of CIO-IT Security-01-02 identifies tools and sources GSA OCISO uses to identify and respond to threat information. They include external entities such as CISA, FireEye Partners, and GSA enterprise network and security monitoring tools.

On a system-by-system basis, individual threat sources/events (e.g., agents, vectors) are identified in accordance with the threat taxonomy in NIST SP 800-30. Additional threat information may be provided by sources such as Continuous Diagnostics and Mitigation (CDM) tools and other automated tools.

4.4 Characterization of Vulnerabilities and Sources

Information system and information security vulnerabilities and predisposing conditions may be identified by the processes described below.

A&A process followed by a GSA system to achieve its initial ATO. All GSA information systems undergo an A&A process leading to an ATO or an approval process leading to an Approval to Use (ATU). Each A&A or approval process described in CIO-IT Security-06-30 requires that an assessment be performed. The assessment may reveal vulnerabilities based on any of the following activities. Any findings resulting from these activities must be assessed for risk.

- Completion of GSA's NIST SP 800-53 test cases associated with the NIST controls required by the system's FIPS 199 categorization and A&A process. This task includes the assessment of information security architectures and integration of security into the development process.
- Vulnerability and configuration scans performed as part of an A&A/approval process as documented in CIO-IT Security-06-30.
- Penetration tests completed as part of a system's A&A process requirements as documented in CIO-IT Security-06-30 and CIO-IT Security-11-51: Conducting Penetration Test Exercises.

Vulnerability management process described in CIO-IT Security-17-80: Vulnerability Management Process. Systems are scanned by various vulnerability scanning tools on a periodic basis as identified in the 06-30 Scanning Parameter Spreadsheet. Various reports (e.g., Top 10 vulnerability summaries, Top 10 Hosts with vulnerability remediation time frames exceeded) are distributed by the ISO division. Verified findings from the scans, as identified in CIO-IT Security-17-80, must be assessed for risk.

Continuous monitoring process described in CIO-IT Security-12-66: **Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program**. Systems in GSA's Ongoing Authorization (OA) Program must adhere to the technical and non-technical assessment of the security controls identified in CIO-IT Security-12-66. Any findings from the automated or manual assessments must be assessed for risk.

Vulnerability Disclosure Policy (VDP). GSA's VDP is publicly available at the VDP web page. This policy establishes a program for security researchers to identify and report vulnerabilities to GSA so they can be remediated.

GSA's CDM implementation in accordance with DHS/Office of Management and Budget (OMB) guidance. GSA has implemented CDM tools per DHS/OMB guidance. As the results of the CDM tools are verified and integrated into GSA's vulnerability and ISCM processes, any findings need to be assessed for risk.

FISMA processes (i.e., annual self-assessments, FISMA metrics analysis) described in CIO-IT Security-04-26: Federal Information Security Modernization Act (FISMA) Implementation. Each fiscal year, OMB and CISA develop FISMA metrics used to oversee Federal agencies' information security policies and practices. FISMA of 2014 requires annual self-assessments, and CISA/OMB require agencies to submit quarterly FISMA security metrics that are compiled into government wide and agency-specific numeric scores aligned to each of the five NIST CSF domains (Identify, Protect, Detect, Respond, Recover). The scores provide a comprehensive picture of an agency's cybersecurity and privacy performance. GSA uses this data to guide the remediation of cybersecurity risks based on requirements in EO 14028, "Executive Order on Improving the Nation's Cybersecurity" and the current Fiscal Year OMB Memorandum on FISMA reporting/Security and Privacy Management Requirements.

Audits (e.g., Inspector General (IG), FISMA) performed on GSA's system and security processes. Audits (internal and external) are performed regularly on GSA systems and security processes. Any audit findings must be assessed for risk.

Incidents/Events identified by internal or external activities. Incidents may be reported by external or internal entities or events may be discovered through network/system monitoring, user reports, or threat intelligence sources. The incident response, monitoring, or threat intelligence actions may identify findings/conditions that need to be assessed for risk. For example, GSA participates in DHS's C-CAR process and complies with DHS Cybersecurity Directives. Both C-CAR and BODs/EDs identify events or vulnerabilities and mandate GSA responses to them.

4.5 Consequences and Impact

At the system level, GSA initially applies the FIPS 199 security categorization to assess the consequences and impacts of risks (i.e., threats exploiting vulnerabilities) to the systems and their data. GSA has also implemented tailored A&A processes and control baselines for

systems that meet additional criteria. For example, systems may qualify for the Lightweight Security Authorization Process or the Low Impact or Moderate Impact Software-as-a-Service Security (LiSaaS/MiSaaS) Authorization processes based on their level of data and environment. Each of these processes have streamlined procedures and controls because the consequences or impact to GSA, individuals, other organizations, and the Nation is reduced.

GSA has specified several NIST SP 800-53 controls as required in addition to the FIPS 199 baselines due to a consideration of GSA's environment, mission, and functions. GSA selected these controls because the consequences and impact of the controls not being implemented correctly, along with a set of Showstopper controls, are too great to allow systems to not implement them. CIO-IT Security-06-30 identifies these additional controls which must be implemented to receive an ATO. For example, all systems that are designated as HVAs, are FIPS-199 High, or are Internet facing must have penetration tests conducted prior to receiving an ATO and annually thereafter.

GSA also mandates controls related to encryption when systems have specific types of information (i.e., PII, Payment Card Industry (PCI), authenticators, system specific business sensitive information) due to the consequences and impact of such data being exposed or the systems breached.

Impact is influenced by factors such as resiliency, spread or containment of an event, the assets susceptible to an event, and weighting factors such as if an asset is listed in GSA's HVA inventory.

4.6 Likelihood

Likelihood is determined manually using data provided by automated tools and system/organizational conditions. As described in NIST SP 800-30, likelihood of an adverse impact is determined by considering:

- How likely is it that threat sources (adversarial or non-adversarial) could cause an event to occur?
- How likely is it, if initiated, that an event would result in an impact?

GSA's robust security stack, including network and endpoint-based solutions, provide information that can inform the answers to the questions above. For example, these tools as well as GSA's threat intelligence may indicate if there are known exploits of vulnerabilities, if the known exploits are readily available, and if there has been evidence of the exploits being used elsewhere or targeted at GSA. Additional tools (e.g., a Governance, Risk, and Compliance [GRC] tool) or additional capabilities in existing tools may provide additional automation of likelihood determination in the future.

4.7 Risk Constraints

The following risk constraints, to some extent, limit GSA's ability to reduce risk:

- Risk remediation is reliant on available resources (e.g., funding, tools/capabilities, personnel) and the effectiveness of those resources in mitigating risk[2].
- Implementation timelines may be impacted by available funding; the complexity of the mitigation; contractual relationships; use of legacy hardware and software; organizational governance structure; geographical location of facilities; legal and regulatory requirements, workforce; organizational culture; and trust relationships.
- Maintaining an accurate inventory of physical and virtual hardware, software, and connections has become difficult with the increased number of mobile devices, the Internet of Things (IOT), and adoption of cloud-based applications and devices.
- The evolving complexity of digital assets has made risk assessment difficult.

4.8 Risk Tolerance

GSA's risk tolerance strategy is based on:

- System categorizations according to FIPS 199 levels.
- System A&A process followed.
- CISO-mandated Showstopper items/associated controls as defined in CIO-IT Security-06-30.
- CISA Cybersecurity Directives.
- Type/sensitivity of data (e.g., PII, other sensitive data, publicly available data).
- Accessibility of the system (i.e., Internet facing or internal access only).

Systems categorized as FIPS 199 High or Moderate typically have a lower risk tolerance than systems categorized as FIPS 199 Low systems with publicly available data. Similarly, systems with PII or other sensitive data have a lower risk tolerance than systems without such data. Systems accessible from the Internet also have a lower risk tolerance, especially if they can be used as an avenue to internal systems. The GSA A&A process a system follows to receive an ATO is, in part, determined by the risks of the system and its data being exploited, which in turn impacts the determination of risk tolerance for the system. For example, a system following the CIO-IT Security-14-68: Lightweight Security Authorization Process has a higher risk tolerance due to the restrictions on the types of systems that can use that process compared to a system following the standard A&A process. CISO Showstopper items/controls that are not fully satisfied may lead to a system not being authorized due to the risk involved and, at a minimum, must have an Acceptance of Risk (AOR) letter approved with a plan on how the risk can be mitigated or resolved. GSA's risk tolerance is summarized by the following statements.

- Risk mitigation is the appropriate risk response for all Very High/Critical and High risk vulnerabilities that can be exploited from the Internet which cannot be accepted, avoided, shared, or transferred.
- Risks from vulnerability scans must be addressed in the following manner:

[2] NISTIR 8286 discusses the use of a risk reserve to avoid or mitigate an identified risk. Risk owners should discuss with acquisition or procurement teams and budget owners the concept of setting aside funding or labor hours as part of a risk reserve during project planning.

(1) BOD Timelines
(a) Within 14 days for vulnerabilities added to CISA's Known Exploitable Vulnerabilities (KEV) Catalog with a common vulnerabilities and exposures (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.

4.9 Priorities and Consideration of Trade-offs

Prioritization of risk response enables a business-driven approach that maximizes the value of GSA's investments. The prioritization of mission functions is established at Level 1 (see Figure 1-1 for Levels) by Executive leadership and communicated to Levels 2 and 3. GSA ranks threat events by the level of risk determined during the risk assessment with the greatest attention going to high risk events impacting:

- Primary Mission Essential Functions (PMEFs): Those mission essential functions that must be performed to support the National Essential Functions before, during, and in the aftermath of an emergency.
- Mission Essential Functions (MEFs): The limited set of agency-level government functions that must be continued throughout or resumed rapidly after a disruption of normal activities.
- HVAs supporting PMEFs and MEFs.

Priority and funding are provided for the implementation of enterprise capability gaps in the Identify, Protect, Detect, Respond and Recover security domains since these capabilities help in preventing emerging threats for all systems supported by the enterprise capabilities. Priorities are adjusted based on changing environment needs. For example, the risks associated with a remote workforce drives the priority for implementation of a zero-trust architecture and model.

GSA has a legal responsibility to protect sensitive information residing on information systems. This includes but is not limited to PII and financial data.

As part of GSA's risk management, trade-offs may be considered. At Level 1, it may be better to aggregate multiple risks in one broad-based response rather than individually addressing each risk. Choosing not to remediate risks on a legacy system scheduled for replacement by instead accelerating completion of the replacement is another example of a trade-off. Risk trade-off decisions are made by the SAORM in consultation with the EMB-Risk Executive (Function).

5 Assessing Risk

GSA's information and information system security risk strategy is based on assessing and managing risks as part of the following processes:

- The A&A process followed by a GSA (Federal or contractor) system to achieve its initial ATO as defined in CIO-IT Security-06-30.
- The vulnerability management process described in CIO-IT Security-17-80.
- The information system continuous monitoring and ongoing authorization processes described in CIO-IT Security-12-66.
- GSA's CDM implementation in accordance with DHS/OMB guidance.
- The DHS HVA assessments of HVA systems.
- The FISMA processes (i.e., annual self-assessments, FISMA metrics analysis) described in CIO-IT Security-04-26.
- Any penetration tests required as defined in CIO-IT Security-06-30 and CIO-IT Security 11-51.
- (OIG), FISMA) performed on GSA's systems and security processes.
- Incidents/Events identified by internal or external activities as described in CIO-IT Security-01-02.
- The POA&M process as defined in CIO-IT Security-09-44.

5.1 Risk Assessments Within GSA

GSA follows the NIST SP 800-30 risk assessment process when assessing information system and information security risks during A&As, essentially following the same steps for the assessments previously identified. That process consists of the following steps and tasks:

- Prepare for Assessment.
- Conduct Assessment.
  - Identify Threat Sources and Events.
  - Identify Vulnerabilities and Predisposing Conditions.
  - Determine Likelihood of Occurrence.
  - Determine Magnitude of Impact.
  - Determine Risk.
- Communicate Results.
- Maintain Assessment.

Preparing for an assessment is unique to the various processes listed earlier (e.g., penetration tests, A&A process, audits) and covered in the GSA IT Security Procedural Guides for those processes and, in general, in CIO-IT Security-06-30 regarding security assessment planning. For these reasons, preparing for the assessment is not covered in this document.

In addition to the process from NIST SP 800-30, "Guide for Conducting Risk Assessments," GSA uses the following processes, as appropriate, for assessing risk:

- Cyber Hygiene/Compliance Assessments (to support implementation of the RMF).
- Software dependency analysis.
- Conventional resilience analysis (e.g., mission resilience or system resilience)
- Assessment of cyber resiliency against advanced cyber adversaries (e.g., the .gov Cybersecurity Architecture Review (govCAR), NSA/CSS Technical Cyber Threat Framework, v2[3], and MITRE ATT&CK™ v12 for Enterprise IT[4]).

[3] "National Security Agency Cybersecurity Report: NSA/CSS Technical Cyber Threat Framework v2," November 2018.
[4] MITRE ATT&CK® v12 Matrix for Enterprise.

All of the risk assessment processes used feed into GSA's overall ERM process and support decision making regarding:

- Development of an information security architecture.
- Definition of interconnection requirements.
- Design, implementation, operation, and maintenance of security solutions.
- Selection of SCRM controls.
- Authorization or denial of authorization to operate information systems.
- Modification of missions/business functions and or processes.
- Funding of information security programs.

5.2 Assessing Risk of External Providers

Many of the assets on which GSA depends are not within its direct control. GSA and its external providers share responsibility for supporting organizational missions and business functions.

FISMA and OMB policies require that federal agencies using external service providers assure that the providers meet the same security requirements that federal agencies are required to meet. GSA utilizes Federal Risk and Authorization Management Program (FedRAMP) approved cloud solutions/service providers and issues Agency FedRAMP ATOs, when appropriate.

As documented in CIO-IT Security-09-48, GSA incorporates the requirement for systems to follow GSA's security processes into the terms and conditions of its IT acquisition contracts. These terms include following the NIST SP 800-37 RMF and implementing NIST SP 800-53 controls for all systems acquired from vendors. GSA requires its external providers to provide appropriate evidence to demonstrate that they have complied with the RMF in protecting Federal information. This includes independent assessments conducted by third parties and continuous monitoring. GSA maintains the responsibility for granting external service providers an ATO.

CIO-IT Security-19-101: External Information System Monitoring requires all external systems to provide evidence that they are following GSA's continuous monitoring processes. The requirements include vulnerability scanning and remediation, configuration management, and periodic deliverables to ensure GSA is able to effectively monitor the security status of external systems. The monitoring of external systems is reinforced by using GSA's implementation of the Archer GRC solution to generate checklists that require ISSOs and ISSMs to indicate if the required monitoring is taking place and any resolution if requirements are lapsing.

5.3 Risk Determination

Risk is determined by both automated and manual methods. Per NIST SP 800-30, risk consists of combining the likelihood of a threat event occurring with the level of impact it would cause. Similar to likelihood, GSA automated tools used as part of the vulnerability management process, CDM implementation, and penetration testing generally provide a risk or vulnerability score based on the results of findings. The DHS risk scoring methodology, Agency-Wide Adaptive Risk Enumeration (AWARE), is used within the CDM tool implementation to provide automation assistance for prioritizing the mitigation of vulnerabilities and risks identified by CDM tools. Manual assessments (e.g., test cases, manual part of penetration tests) will have risk determined manually. A more detailed description of how information system risks are assessed is provided in CIO-IT Security-06-30.

Note: A tool's risk rating is not necessarily the final risk rating for a vulnerability and its possible exploitation. Other factors, such as the environment where the vulnerability exists, automated or manual safeguards that provide additional protection, etc. may cause assessors to raise or lower the risk of a threat event causing an adverse impact.

As described in Section 4.4., DHS/OMB compile agencies' FISMA metrics into agency-specific scores aligned to each of the five NIST CSF domains. GSA considers the OMB/CISA scores and their underlying data as part of its risk remediation and mitigation process. GSA also uses input from the annual FISMA OIG audit, financial audits, and other third-party audits as part of determining risk and its remediation and mitigation. Every audit finding generates a POA&M that is monitored until resolution.

6 Responding to Risk

GSA considers the following types of possible responses to risk when identifying, evaluating, and deciding on courses of action: risk acceptance, risk avoidance, risk mitigation, and risk sharing. Details regarding these courses of action are discussed in Section 6.3.

At each level in Figure 1, responses to risk are managed using different tools and processes. At the system level, risks are managed by responding to identified vulnerabilities and risks and, when necessary, entering them into a system level POA&M that is used to monitor and track the risk. At the business process/program level, risks are managed by a Program level POA&M and the activities identified in CIO-IT Security-08-39 and the quarterly AO Sync meetings established therein. In AO Sync Meetings, senior managers within GSA's organizations see how their systems are performing in responding to risk, and decisions can be made concerning prioritizing specific risk responses. At the Agency level, the ERSI Board and the EMB establish responses to enterprise risks and monitor and track them as part of their charters. The EMB uses a risk profile and risk management action plans for monitoring risks. The GSA CISO has established a Cybersecurity Risk Register (see Appendix D) to track and monitor cyber risks and to identify if risks should be presented to the ESRI.

6.1 Risk Response Identification

As described in previous sections, risks are identified and assessed using various tools, processes, and from input from sources such as audits and third-party assessments. The responses to risks at levels 2 and 3 are governed by processes described previously, such as requirements specified in CIO-IT Security-06-30 regarding vulnerability remediation timeframes and acceptance of risk, the activities documented in CIO-IT Security-08-39 that address requirements from various other Federal and GSA guidance documents such as Executive Orders, BODs/EDs, and GSA's vulnerability management process. The responses at Level 1 are governed by the GSA ERSI Board and EMB.

6.2 Evaluation of Alternatives

At each level, alternative courses of action are identified for all risks above the risk tolerance, sequentially starting with the highest risks. Alternative courses of action may include implementing compensating controls, updating operational procedures, implementing technical changes using existing capabilities, developing, or acquiring new solutions, designing architectural changes, and/or changes in organizational culture or programs.

GSA's evaluation of alternative courses of action includes considering 1) the expected effectiveness in achieving the desired risk response (and how effectiveness is measured and monitored) and 2) the anticipated feasibility of implementation, including, for example, mission/business impact, political, legal, social, financial, technical, and economic considerations.

GSA, as a provider of many shared services for other Government agencies, cannot assume the risk for other agencies using GSA's systems. Those agencies using GSA's systems must make their own risk-based decision, following their processes, before using the systems.

6.3 Risk Response Decision

Risk-informed decisions (e.g., risk response) enhance mission accomplishment by reducing the loss or degradation of confidentiality, integrity, or availability. Risk response decisions are made at the appropriate level. At the system level, AOs and the CISO are cognizant of risk responses based on system artifacts, which may include Security Assessment Reports (SARs), POA&Ms, and AORs. At the business process/program level, the CISO AOs, and others they designate, are involved in establishing risk responses that address multiple systems, up to and including the enterprise. At the enterprise level the CISO and ERSI and EMB board members make decisions that affect the enterprise and impact the other levels.

The following sections discuss the various decisions that may be made to address risks.

6.3.1 Risk Acceptance

The acceptance of risk for GSA systems is initiated by the discovery of vulnerabilities or findings from GSA's A&A, vulnerability management, and continuous monitoring processes, or as the result of an internal or external audit. Depending on the nature and characteristics of specific risks, the acceptance of risk is governed by either GSA's standard process for risk acceptance or GSA's CISA KEV process for risk acceptance.

6.3.1.1 GSA Standard Risk Acceptance Process

Per CIO-IT Security-06-30, Critical (Very High) and High risk vulnerabilities must be remediated within 30 days; moderate risk vulnerabilities must be remediated within 90 days; and Low risk vulnerabilities on Internet-accessible systems/services must be remediated within 120 days.

Vulnerabilities that cannot be remediated within the timeframes listed above may have the risk accepted as follows:

- Very Low/Low risks – risk is accepted with no AOR letter required.
- Moderate risks - acceptance is by the AO and IST and ISO Directors approving a Moderate risk AOR Letter.
- Critical (Very High)/High risks – acceptance is by the AO and IST and ISO Directors approving a Critical/High risk AOR Letter with CISO concurrence.

AOs may issue an ATO with conditions when risks have not been remediated with the length of the ATO predicated on a timeline to remediate the risks and vacate the conditions of the ATO.

CIO-IT Security-06-30 provides additional details on AOR Letters and the circumstances under which they may be issued and the process for their request and approval. Typical conditions for which AOR letters may be approved include:

- The system has budgetary constraints that limit remediation efforts.
- The system is a legacy system that cannot be patched.
- The system is scheduled for disposal.

6.3.1.2 GSA CISA KEV Risk Acceptance Process

Vulnerabilities published in CISA's KEV Catalog pose significant risk to GSA's systems and information. Tracking of CISA KEV vulnerabilities that have not been remediated and AOR Letters associated with them will be addressed by the following process.

1. A standing AOR for any non-remediated KEV CVE that exceeds 29 days and is less than 89 days will be created for each business line, as necessary.
    a. KEVs under this AOR will be tracked within business line's KEV AOR tracking sheet.
        i. A POA&M ID and related AOR information will be associated with each KEV CVE tracked in the sheet.
        ii. KEV CVEs that have been remediated will be identified as remediated but will remain in the tracking sheet.
    b. KEV AORs will be tracked on a weekly basis by the GSA CISO and AOs will be briefed at least quarterly on their business line's KEV AOR status.
2. Any non-remediated KEV CVE that exceeds 89 days will either:
    a. Have a specific AOR created for it, or
    b. Have affected assets removed from the network.

6.3.2 Risk Avoidance

Risk avoidance occurs when the appropriate risk is deemed to exceed the organizational risk tolerance. If risk avoidance is used for any particular risk, specific actions must take place to eliminate the activities or technologies that are the basis for the risk.

GSA uses risk avoidance for all technologies that have Very High/Critical or High vulnerabilities that can be exploited from the Internet but cannot be mitigated. For example, end-of-life (EOL) software can be avoided if, during system design, the architecture and software inventory is reviewed for existing or soon-to-be EOL software.

6.3.3 Risk Mitigation

Risk mitigation is the appropriate risk response for all Very High/Critical and High risk vulnerabilities that can be exploited from the Internet and cannot be accepted, avoided, shared, or transferred. Risk mitigation measures are employed based on prioritization. In general, the prioritization aligns with the level of risk (i.e., Very High/Critical risks should be addressed prior to High risks); however, when there are multiple risks at the same level, system, and security personnel coordinate to establish which risks will be addressed first. Prioritization is typically a manual process including criteria such as the probability of vulnerability exploitation, material business impact if vulnerability is successfully exploited, compliance requirements, evaluation of attack vectors and exposures, level of assets (i.e., High Value and Critical assets prioritized above others), and the cost and business impact of remediation activities and controls. The DHS AWARE process will assist in automating prioritization for risks identified as part of the CDM program.

The mitigation of risks identified in DHS BODs/ EDs or from the C-CAR protocols is prioritized based on the risk levels and timelines specified by DHS.

6.3.4 Risk Sharing or Transfer

GSA uses risk sharing or risk transfer when GSA and other agencies or vendors are responsible for different pieces of the hardware or software stack. Contractor Owned/Contractor Operated (COCO) and cloud-based systems meet these criteria.

Risk is also shared when a system is a subsystem of another system, when controls are inherited as common or hybrid controls from the enterprise or other systems, and when any as-a-service offering is used. In all cases, the two systems share risk based on their reliance on each other for implementing part or all of a control.

When GSA systems interconnect with another organization's or vendor's systems the risks are shared and described in the associated Interconnection Security Agreement (ISA)/Information Exchange Agreement (IEA).

6.4 Sharing Risk-Related Information

At the enterprise level, GSA uses the EMB, serving as the Risk Executive (Function), to share risk-related information with key GSA personnel. The GSA CISO uses a Cybersecurity Risk Register (see Appendix D) to aggregate and manage the organization's highest cybersecurity risks in a consistent, structured manner. Inputs to the Cybersecurity Risk Register include A&A assessments/POA&Ms, audit findings, and findings from BODs/EDs, and other third-party assessments.

The EMB (of which the CIO is a member), in consultation with the ERSI Board (of which the CISO is co-Chari) determines which risk information can be shared externally. The CDM and FISMA reporting processes require certain risk related information to be shared with CISA and OMB. Any risks arising from the CDM and FISMA reporting processes are communicated with the GSA Administrator and Deputy Administrator by the CIO and CISO.

7 Monitoring Risk

Ongoing monitoring is a critical part of the risk management process. GSA uses risk monitoring to:

- Verify compliance with information security requirements.
- Determine the ongoing effectiveness of risk response measures.
- Identify changes to information systems and environments of operation that may impact the risk posture.

7.1 Monitoring Compliance

Compliance monitoring ensures that cybersecurity controls at Levels 1, 2, and 3 have been implemented correctly and are operating as intended. Compliance monitoring also verifies that the information security requirements are derived from and traceable to GSA's missions, business functions, federal legislation, directives, regulations, policies and standards, and guidelines.

GSA conducts compliance monitoring to verify continued control implementation after the initial assessment of the system per the RMF. GSA's compliance monitoring relies on automation as much as possible and includes:

- Vulnerability management processes described in CIO-IT Security-17-80.
- Continuous monitoring processes described in CIO-IT Security-12-66.
- GSA's CDM implementation in accordance with DHS/OMB guidance. Dashboards are used to monitor vulnerabilities and configuration setting compliance.
- FISMA processes (i.e., annual self-assessments, FISMA metrics analysis) described in CIO-IT Security-04-26.
- Audits (e.g., IG, FISMA, third-party) performed on GSA's system and security processes.
- Incidents/Events identified by internal or external activities described in CIO-IT Security-01-02.
- AO Sync meetings as described in CIO-IT Security-08-39.

The use of these tools and processes is facilitating GSA's 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.

7.2 Monitoring Effectiveness

Monitoring the effectiveness of GSA's risk management strategy is gauged by evaluating how effective implemented risk response measures, including the implementation of any remediation or compensating controls, have been in reducing identified risks to the desired level. GSA initially monitors the effectiveness of its risk management framework before a system goes into production via the A&A ATO process and through analyzing the results of the processes in the following guides.

- CIO-IT Security-04-26 – requiring annual FISMA self-assessments and collaborating on FISMA metric reports.
- CIO-IT Security-06-30 – requiring initial ATOs and specific controls such as vulnerability scanning, configuration management, continuous monitoring, and periodic updates of A&A documents.
- CIO-IT Security-08-39 – identifies recurring activities systems must perform (e.g., resolve vulnerabilities, manage POA&M resolution, maintain A&A documents, including the AO Sync meetings where the CISO and AOs monitor compliance with the required activities.
- CIO-IT Security-09-44 – monitoring the progress in resolving POA&Ms, including POA&Ms associated with AORs and ATO contingencies.
- CIO-IT Security-12-66 – using CDM and other enterprise security tools to monitor systems security posture and documentation updates.
- CIO-IT Security-17-80 – scanning for vulnerabilities and checking configuration setting compliance.
- CIO-IT Security-19-95: Security Engineering Architecture Reviews – requires initial and periodic architecture reviews for security implementations.
- CIO-IT Security-19-101 – requires periodic checks on the security posture of vendor/contractor systems and the maintenance of security documentation.

These processes provide key insight into how GSA's risk management strategy is performing. Effectiveness monitoring is also performed by defining key performance metrics/indicators, defining acceptable thresholds for the indicators, and measuring progress towards achieving the performance metrics.

Based on the analysis of the effectiveness of these risk management processes, metrics, and measures, GSA modifies them in order to reduce risks and improve information system and information security. Modifications may include, but are not limited to, the following types of actions:

- Increasing automation (e.g., security orchestration tools) in identifying vulnerabilities and risks, including improving and expanding the use of dashboards.
- Modifying measures/metrics to increase expected levels of protection of systems and their data.
- Improving incident response and vulnerability detection capabilities by assessing new tools, technologies, and techniques, and integrating them where appropriate.
- Modifying GSA's VDP to improve the identification and remediation of vulnerabilities.
- Focusing remediation/mitigation responses to address the highest risk/highest impact items first.
- Using lessons learned during response and recovery activities/tests to improve processes and techniques.

7.3 Monitoring Changes

Change monitoring is a component of the change management process, which manages updates to production systems. Changes to systems are overseen through GSA's change and configuration management processes. However, those changes which affect prior risk decisions, like changes in the value of information, threat environment, technologies used, or the use of an end-of-life product, can affect the security state of the system and are carefully monitored by GSA.

8 Communicating Results

The results of risk assessments and overall risk management are communicated using multiple methods. The primary means used are:

- **Security Assessment Reports (SAR).** SARs are prepared as part of a system's A&A process and include all risks determined as part of the assessment. Certain A&A processes (defined in CIO-IT Security-06-30) will not have a formal SAR, but they will still assess risk as part of an assessment of the system.
- **Penetration Test Reports (when required).** Systems required to have a penetration test performed will receive a penetration test report communicating the results of the penetration test for analysis and risk management.
- **Dashboards.** GSA's automated tools (CDM and vulnerability scanning) include dashboards or similar features where authorized personnel can review risk results from the automated tool assessments, including the ISCM dashboard in GSA's Elasticsearch, Logstash, Kibana (ELK) stack.
- **Plan of Action and Milestones (POA&M).** POA&Ms are required for every system at GSA. Subsystems, as defined in CIO-IT Security-06-30 typically have their POA&Ms included in the FISMA system they reside on. In special situations, after coordination with the OCISO, they may have their own POA&M. GSA's POA&M process is described in CIO-IT Security-09-44 and includes reports on the effectiveness of POA&Ms in managing and mitigating risks. Reports are provided to personnel responsible for the security of individual systems, with summary reports provided to GSA ISSMs, IS Directors, and the CISO.

- **AO Sync Meetings.** These meetings provide a feedback mechanism to inform AOs about how well the systems under their purview are performing regarding risks. The quarterly briefings provide a practical tool with which AOs can gauge the effectiveness of their information security arrangements and assess how well their systems are performing.

8.1 Sharing Risk-Related Information

Sharing of risk-related information within GSA (but outside of IS) is at the determination of the CISO in collaboration with AOs, ISSMs, IS Directors, and subject matter experts within the OCISO. Part of the collaboration described is to determine which risks are appropriate to become a part of the GSA CISO's Cybersecurity Risk Register and, if appropriate, forwarded for ERSI consideration.

The CISO, in consultation with the IS Directors and GSA Executive Management, makes the determination on what risk information should be shared externally. The separate CDM and FISMA reporting processes require certain risk related information be shared with DHS and OMB by law and Federal regulation. Any risks arising from the CDM and FISMA reporting processes (e.g., FISMA IG audits, RMA reports) are communicated with the GSA Administrator and Deputy Administrator by the GSA CIO and CISO.

9 Monitoring Risk Factors

Risk factors, such as threat sources, vulnerabilities, etc., are monitored by the assessment processes described earlier. The ISO Division updates threat information as part of the Threat Awareness Program described in CIO-IT Security 01-02. Vulnerabilities are monitored via GSA's assessment and continuous monitoring processes, some of those processes occur as often as weekly, others annually, and others as an A&A or security assessment process requires.

9.1 Updating Risk Assessments

Similar to the monitoring of risk factors, updating of risk assessments occurs dependent upon the A&A process being followed. POA&Ms are expected to be maintained regularly as new vulnerabilities/risks are identified, and as actions within the POA&M are performed. POA&Ms are required to be updated at least quarterly. Automated tools (CDM, vulnerability scanners) identify new vulnerabilities/risks and whether or not previous vulnerabilities/risks have been resolved. The vulnerabilities the automated tools check for are updated on a regular basis by the tool vendors, details are in CIO-IT Security-17-80.

9.2 Response to Change

GSA monitors changes to its information systems and their architectures by periodically assessing risks at the mission/business process levels in which those systems operate.

- **Information System:** Changes that occur in GSA information systems (including hardware, software, and firmware) may introduce new risk or change existing risk. GSA has established a rigorous configuration change management process. Any IT changes are requested through a defined CM approval process (e.g., a chartered Change Control Board [CCB]) using automated or manual processes to document the nature of changes, their criticality, impacts on the user community, testing and rollback procedures,

stakeholders, and points of contact. System changes are tested and validated prior to implementation into the production environment. Configuration settings and configuration baselines are updated as necessary to meet new technical and/or security requirements and are controlled through the CM process. The CM process requires testing/validating changes where the scope of the change has a major impact on agency reputation, has a large scope or has the potential for significant monetary impact. Additional details on change management can be found in CIO-IT Security-01-05: Configuration Management (CM).

- **Environments of Operation:** Environmental and operational considerations include, but are not limited to, missions/business functions, threats, vulnerabilities, mission/business processes, facilities, policies, legislation, and technologies.

10 Aligning NIST Risk Assessments and the CSF

As described in the introduction, GSA adheres to NIST guidance as it relates to risk management. All of GSA's A&A processes have the NIST RMF as a foundation. Risk assessments are performed in accordance with NIST SP 800-30. GSA manages, tracks, and submits FISMA metrics and performance measures which are aligned to the CSF core functions to inform risk management decisions and planning. As required by EO 13800, GSA has aligned its risk management process with the NIST CSF core functions as described below.

Identify (ID): Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

- GSA has identified its high value/critical assets which guides how GSA prioritizes risk resolution.
- Vulnerabilities are identified and documented, including threats, likelihoods, and impacts, via the multiple processes listed at the beginning of Section 5.
- The ISE Division receives threat intelligence from multiple sources and communicates this information to GSA's information security community.
- As part of this document and CIO-IT Security-06-30, risk prioritization and tolerance are identified.
- Systems categorized as FIPS 199 High or Moderate typically have a lower risk tolerance than systems categorized as FIPS 199 Low systems with publicly available data.

Protect (PR): Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

- GSA's adherence to the NIST RMF process guides how systems are protected by security categorization, security control selection and implementation, and remediation of risks to protect systems.
- CIO-IT Security 17-80 and CIO-IT Security-12-64: Physical and Environmental Protection (PE) provide processes for managing vulnerabilities to address where additional protection is needed.

Detect (DE): Develop and implement appropriate activities to identify the occurrence of a cybersecurity incident.

- Vulnerabilities may be detected and documented, including threats, likelihoods, and impacts, via the multiple processes listed at the beginning of Section 5.

- Incidents and events may be detected by GSA's perimeter defenses such as firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), or the Enterprise Logging Platform (ELP).
- Users may detect unusual or abnormal items or behavior in systems or applications (e.g., phishing emails) and report them to the IT Helpdesk.

Respond (RS): Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

- As incidents are responded to in accordance with CIO-IT Security-01-02, risks based on the incidents and vulnerabilities exploited will be shared as appropriate.
- As part of incident after action/lessons learned reports and semi-annual testing of the incident response plan, the plan, and processes within it are updated to improve future response actions.

Recover (RC): Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Although recovery is generally not a part of assessing risks, lessons learned during recovery from incidents provide feedback that can be used to improve response and recovery processes and reduce risks in the future. CIO-IT Security-06-29: Contingency Planning (CP) requires GSA systems to have a contingency plan, including a Business Impact Assessment (BIA), which must address system recovery and restoration of operations.

For more information on GSA's alignment of the RMF to the CSF, refer to CIO-IT Security-06-30.

Appendix A: References

Note: GSA updates its IT security policies and procedural guides on independent cycles which may introduce conflicting guidance until revised documents 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.

The following references provide guidance, mandates, or direction on managing information system, security, and privacy risk within GSA.

Federal Laws, Standards and Guidance:

- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Directives
- EO 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- EO 14028, "Executive Order on Improving the Nation's Cybersecurity"
- Federal Financial Management Improvement Act of 1996 (FFMIA)
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST Cybersecurity Framework, Version 1.1, Framework for Improving Critical Infrastructure Cybersecurity (NIST web page on Cybersecurity Framework)
- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments"
- 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 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"
- NISTIR 8286, "Integrating Cybersecurity and Enterprise Risk Management (ERM)"
- NISTIR 8286A, "Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)"
- OMB Circular A-123/OMB Memo M-16-17, "Management's Responsibility for Enterprise Risk Management and Internal Control"
- OMB Circular A-130, "Managing Information as a Strategic Resource"
- OMB Memo 16-24, "Role and Designation of Senior Agency Officials for Privacy"
- Current Fiscal Year OMB Memorandum on FISMA Reporting, "FYxx FISMA Guidance" or "Fiscal Year xxxx Guidance on Federal Information Security and Privacy Management Requirements"
- Public Law 113–283, "Federal Information Security Modernization Act of 2014''

GSA Directives, Policies, and Procedures:

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

The following guides are available at gsa.gov on the IT Security Procedural Guides webpage.

- CIO-IT Security-01-02: Incident Response (IR)
- CIO-IT Security-01-05: Configuration Management (CM)

- CIO-IT Security-04-26: Federal Information Security Modernization Act (FISMA) Implementation
- CIO-IT Security-06-29: Contingency Planning (CP)
- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-08-39: [Current FY] IT Security Program Management Implementation Plan
- CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts
- CIO-IT Security-11-51: Conducting Penetration Test Exercises
- CIO-IT Security-12-64: Physical and Environmental Protection (PE)
- CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program.
- CIO-IT Security-14-68: Lightweight Security Authorization Process
- CIO-IT Security-17-80: Vulnerability Management Process
- CIO-IT Security-19-95: Security Engineering Architecture Reviews
- CIO-IT Security-19-101: External Information System Monitoring

Appendix B: Acronyms

Acronym	Description
A&A	Assessment & Authorization
AWARE	Agency-wide Adaptive Risk Enumeration
AO	Authorizing Officials
AOR	Acceptance of Risk
ATO	Authorization to Operate
ATU	Authorization to Use
BOD	Binding Operational Directive
C-CAR	Cybersecurity Coordination, Assessment, and Response
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CO	Contracting Officer
C-SRM	Cyber Supply Chain Risk Management
CSRM	Cybersecurity Risk Management
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
ED	Emergency Directive
ELK	Elasticsearch, Logstash, Kibana (i.e., ELK stack)
ELP	Enterprise Logging Platform
EMB	Enterprise Management Board
EO	Executive Order
EOL	End of Life
ERM	Enterprise Risk Management
ERSI	Enterprise Risk and Strategic Initiatives
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
govCAR	.gov Cybersecurity Architecture Review
GRC	Governance, Risk, and Compliance
HSSO	Head of Services and Staff Offices
HVA	High Value Assets
IA	Information Assurance
IDS/IPS	Intrusion Detection Systems/Intrusion Prevention Systems
IG	Inspector General
IR	Incident Response
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISE	GSA OCISO Security Engineering Division
ISI	Identity, Credential, and Access Management (ICAM) Share Service Division
ISO	GSA OCISO Security Operations Division
ISP	GSA OCISO Policy and Compliance Division
ISSO	Information System Security Officer
ISSM	Information System Security Manager
IST	GSA OCISO ISSO Support Division
IT	Information Technology
LATO	Lightweight Security Authorization Process

Acronym	Description
LiSaaS	Low Impact Software-as-a-Service
MEF	Mission Essential Functions
MIP	Management Implementation Plan
MiSaaS	Moderate Impact Software-as-a-Service
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OMB	Office of Management and Budget
OA	Ongoing Authorization
PCI	Payment Card Industry
PII	Personally Identifiable Information
PMEF	Primary Mission Essential Functions
POA&M	Plan of Action and Milestones
RMA	Risk Management Assessment
RMF	Risk Management Framework
SAA	Security Advisory Alerts
SAR	Security Assessment Report
SAOP	Senior Agency Official for Privacy
SAORM	Senior Accountable Official for Risk Management
SDLC	System Development Life Cycle
SP	Special Publication
SSO	Services and Staff Offices
VDP	Vulnerability Disclosure Policy

Appendix C: Glossary

The definitions of the terms listed are from the NIST online glossary, unless otherwise noted.

Term	Definition
Availability	Ensuring timely and reliable access to and use of information.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
Cybersecurity Risk	An effect of uncertainty on or within a digital context. Cybersecurity risks arise from the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (e.g., mission, functions, image, reputation) and assets, individuals, other organizations, and the Nation.
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information, and mission management.
High Value Asset (HVA)	A designation of Federal information or a Federal information system when it relates to one or more of the following categories: - Informational Value – The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries. - Mission Essential – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system. - Federal Civilian Enterprise Essential (FCEE) – The information or information system serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.
Impact	With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.
Information Security	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. [Note: The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Likelihood of Occurrence	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.
Mission Essential Functions	The essential functions directly related to accomplishing the organization's mission as set forth in its statutory or executive charter. Generally, MEFs are unique to each organization. FEMA.gov
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., a Federal agency or, as appropriate, any of its operational elements).
Plan of Action and Milestones	A document for a system that "identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Primary Mission Essential Functions	Primary Mission Essential Functions (PMEFs) are those functions that need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations can be resumed. PMEFs are validated by the Federal Emergency Management Agency (FEMA) National Community Coordinator. DHS.gov
Residual Risk	Risk that remains after risk responses have been documented and performed.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Appetite	The broad-based amount an enterprise is willing to accept in pursuit of its mission/vision.
Risk Executive (function)	An individual or group within an organization, led by the senior accountable official for risk management, that helps to ensure that: security risk considerations for individual systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and managing risk from individual systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Register	A repository of risk information including the data understood about risks over time.
Risk Tolerance	The organization's or stakeholder's readiness to bear the remaining risk after risk response in order to achieve its objectives, with the consideration that such tolerance can be influenced by legal or regulatory requirements.
Senior Accountable Official for Risk Management	The senior official, designated by the head of each agency, who has vision into all areas of the organization and is responsible for alignment of information security management processes with strategic, operational, and budgetary planning processes.
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

System Development Life Cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix D: Cybersecurity Risk Register

GSA's Cybersecurity Risk Register is maintained in a Google Sheet. Access to this sheet is restricted due to the sensitivity of the data. The register was adapted from NISTIR 8286.

GSA updates the risk register, at a minimum, on a biannual basis. The fields in the risk register are summarized below, additional information is provided in the Google Sheet.

Table D-1. Cybersecurity Risk Register Fields

Field	Description
ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register.
Priority	A relative indicator of the criticality of this entry in the risk register.
Risk Tier	The tier within the enterprise risk management process where the risk resides (Enterprise, Program/Business Line/Organization, Operations/System).
Risk Area	The risk area for the identified risk.
Operational Risk Statement	A brief description of the operational risk to GSA and other organizations.
Risk Description	A brief explanation of the cybersecurity risk scenario.
Elevate to ERSI?	Recommendation on whether the risk should be elevated to ERSI Board (Yes, No).
Risk Category	An organizing construct that enables multiple risk register entries to be consolidated.
Impact	The potential consequences resulting from this scenario if no additional response is provided.
Likelihood	The estimation of the probability, before any risk response, that this scenario will occur.
Risk Rating	A calculation of the likely risk exposure based on the inherent likelihood estimate and the determined benefits or consequences of the risk. (Very High, High, Moderate, Low, Very Low).
Risk Response Type	The risk response (sometimes referred to as the risk strategy or risk treatment) for handling the identified risk.
Risk Response Cost	The estimated cost of applying the risk response
Risk Response Description	A brief description of the risk response.
Risk Owner	One or more parties that are responsible for managing and monitoring the selected risk response
Status	The current condition of this risk.

GSA aggregates, normalizes, and prioritizes risks in the cybersecurity risk register against risks identified in other risk registers like program management risk, budgetary risk, and legal liability risk. The resulting document is called a risk profile. GSA uses the risk profile to choose which enterprise risks to address and then to delegate responsibilities to appropriate risk owners.