HIGH VALUE ASSET CONTROL OVERLAY

Version 2.0

January 2021

Cybersecurity and Infrastructure Security Agency

Table of Contents

Introduction

Background

The Federal High Value Asset (HVA) initiative was established to identify, assess, and secure the Chief Financial Officers (CFO) Act and Non-CFO-Act agencies' most critical information systems. In 2018, the Office of Management and Budget (OMB) released Memorandum (M) 19-03 to provide guidance on the enhancement of the HVA Program and providing agencies the following guidance allowing greater flexibility in the identification and designation of their most critical assets:

An agency may designate federal information or a federal information system as an HVA 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.[1]

This HVA Control Overlay (Overlay) version 2.0 was developed by the HVA Program Management Office (PMO) to provide technical guidance to federal civilian agencies to secure HVAs. The purpose of this document is to specify controls that agencies should implement to adequately protect their HVAs. These controls were selected based on HVA risks and vulnerabilities identified across the Federal Government as part of the overall efforts to manage and reduce cybersecurity risks.

The Cybersecurity and Infrastructure Security Agency (CISA) was established with the mission to "lead the National effort to understand and manage cyber and physical risk to our critical infrastructure."[2] A component of that mission is to ensure appropriate protections and controls are implemented to secure the Nation's most critical assets. The first iteration of the Overlay was published in November 2017. Since then, CISA has conducted over 50 assessments on HVAs and gained key insights into the cybersecurity posture of the Federal HVA Enterprise (FHE). Additionally, the cybersecurity community has gained working knowledge of emerging technologies and their associated risks. This updated version of the Overlay intends to reflect insights and lessons learned to provide the most effective recommendations and best enhancements to HVA security. This version of the Overlay is aligned with the final version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 5 published in September 2020. [3]

[1] "Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program," Office of Management and Budget, Memorandum M-19-03, 2018
https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[2] "About CISA," Department of Homeland Security Cybersecurity and Infrastructure Security Agency, accessed June 12, 2020
https://www.cisa.gov/about-cisa

[3] As of the release date of this version of the Overlay, the final version of NIST SP 800-53 Rev 5 has been published.

Fiscal Year 2020 HVA Control Overlay Scope and Updates

The fiscal year (FY) 2020 (20) release of the Overlay includes controls and associated enhancements based on the results of **HVA assessments conducted by CISA, combined with up-to-date threat intelligence and cybersecurity trends.** The Overlay's control selections are based solely on these criteria to assist agencies with cyber risk management of their HVA enterprise. Selection of these controls is not contingent upon the latest release of the security control source documents. The mapping of controls to NIST SP 800-53 is intended to provide a reference to the common list of controls in the NIST publication.

> The Overlay's controls and enhancements protect against risks and trends identified through past and present HVA assessments, including Risk Vulnerability Assessments and Security Architecture Reviews, and other risk areas identified by HVA PMO that directly impact federal HVAs.

Controls have been selected and enhanced where appropriate to reduce the following risks:

- size of threat vectors and attack surface;
- ability of unintended lateral movement from adjacent components through lack of segmentation and strict flow control;
- unauthorized system access;
- unintended network and system permissions in access control to include privileged accounts;
- data shared outside the HVA authorization boundary;
- data shared over interconnections and increased risk of the loss of confidentiality outside the authorization boundary;
- device audit and logging information not being centralized for ease of protection to facilitate monitoring to improve capabilities to detect threats;
- security risks involved in the acquisition supply chain for devices supporting HVAs;
- incomplete security of personally identifiable information (PII) present on and processed by the HVA; and
- the lack of transparency of HVA security as it relates to the needs of all stakeholders.

The Overlay specifies security control implementations to make HVAs more resistant to attacks, limit the damage from attacks when they occur, and improve resiliency and survivability. The components of the Overlay provide a defense-in-depth approach which limits and monitors access to critical components to provide protection from the loss of confidentiality, integrity, and availability.

Applicability

HVAs and Non-HVAs

The primary focus of the Overlay is to provide additional instructions on securing federal HVA systems as defined in OMB M-19-03. These controls should be applied on an as-needed basis when evaluating the security of HVA and non-HVA systems to at least a moderate level baseline.[4] This Overlay may be used in full or in part to protect systems against cyber threats. The Overlay does not apply to National Security Systems (NSS) for which system operators should follow the appropriate compliance and organizational standards. The Overlay focuses on control guidance applicable to

[4] For a more detailed breakdown of security control baselines, please reference the latest version of NIST SP 800-53B, https://csrc.nist.gov/publications/detail/sp/800-53b/final.

HVAs but does not provide exhaustive detail for each control.[5] As mentioned in previous sections, these controls were selected based on CISA assessments of HVAs beginning in FY16, recent cybersecurity trends, and threat intelligence available to CISA.

Emerging Technologies

In addition to the existing security concerns related to current technologies, there are progressive system advancements and potential associated risks that have not yet been fully identified. To address some of the concerns and risks associated with these advancements. The section below introduces some of the emerging technologies that may be relevant to HVAs and federal information systems at the present or in the future.

5G

Fifth Generation (5G) is a network to be used by a variety of wireless communications systems with the ability to process much more data than the previous networks. “Many 5G systems will operate at much higher (millimeter wave) frequencies and offer more than 100 times the speed and data-carrying capacity of today’s cellphones, all while connecting billions of mobile broadband users in ever-more-crowded signal environments.”[6]

Although this new technology has benefits to include increased speed and availability of information, there are also associated risks and security concerns. Standards and best practices to address these risks and concerns should be considered prior to deployment. The application of 5G, specifically in HVA environments, presents several risks. The dramatically increased movement and processing of data that 5G allows will further challenge system owners’ already stressed capacity in protecting their HVAs’ data. 5G requires that HVAs implement modernized security measures which rely on – for example – strict connection policies, boundary protection, and advanced access controls. Additionally, agencies will need to fully comprehend their HVA network topology and data flow within that network to effectively identify malicious activity. As stated in NIST’s project description, *5G Cybersecurity, Preparing a Secure Evolution to 5G*, “The National Cybersecurity Center of Excellence (NCCoE) is initiating an effort in collaboration with industry to secure cellular networks and, in particular, 5G deployments. The NCCoE is positioned to promote the adoption of the increased cybersecurity protections 5G networks provide, such as the addition of standards-based features and the increased use of modern information technologies, including the cybersecurity best practices they provide.”[7]

In 2020, the Executive Branch of the United States Government identified 5G in the *National Strategy to Secure 5G of the United States of America* as an emerging technology that malicious actors are already seeking to exploit.[8] The Federal Government’s priorities are to secure the 5G network in the United States while assessing and addressing risks prior to global 5G development and deployment. agencies intending to utilize 5G for HVA systems or components may use the Overlay, the cybersecurity practices and standards defined by NIST and the National Strategy as

[5] For a full discussion of each control please review NIST SP 800-53 Rev 5.

[6] “What is 5G?”, Advanced Communication, National Institute of Standards and Technology, June 2019, https://www.nist.gov/topics/advanced-communications/what-5g

[7] “5G Cybersecurity, Preparing a Secure Evolution to 5G” National Institute of Standards and Technology, April 2020, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/5G-pse-project-description-final.pdf

[8] “National Strategy to Secure 5G of the United States” Executive Branch of the United States Government, March
2020, https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf

resources to protect those systems.

Artificial Intelligence

Artificial Intelligence (AI) has rapidly emerged as a technology with a broad array of potential capabilities across the federal and private sectors. According to NIST, AI has the capability to revolutionize the way the Federal Government and the private sector does business.[9] AI is a "…branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement."[10]

In recognition of AI's potential, the President signed Executive Order (EO) 13859 in February 2019 which outlines the national strategy on AI. The goal of EO 13859 is to promote and secure the development of AI in the Nation and to leverage AI to help the Federal Government provide services and achieve its missions.[11] AI carries risks along with the benefits; however, those risks are not unique to AI and may be related to those that face the broader federal enterprise.

The Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) published a study in 2018 that identified some of these risks and factors to consider when developing standards to address these risks. The study found that, without proper AI-oriented training and education, users may fall prey to adversaries that may exploit AI or use AI to exploit vulnerabilities.[12] The study also noted data integrity may be especially vulnerable because data is sometimes used to train AI to improve performance. Adversaries may exploit AI's reliance on data by injecting malicious or corrupt data into the system which may result in degraded system performance. In addition, the open nature of AI development allows for a freer exchange of knowledge and ideas, but it may also increase the risk of threat actors obtaining AI resources. NIST also published a response and corresponding plan to carry out EO 13859 in August 2019, in which additional standards that may apply to AI development and use were addressed.[13] These standards include requirements for networking, privacy, and risk management. The updated Overlay provides controls for each of these core elements and can be used as a tool for agencies to approach AI development and use with respect to their HVAs.

The Executive Branch of the United States Government issued *Guidance for Regulation of Artificial Intelligence Applications*, which requires federal agencies continue to develop AI while incorporating security controls to "…ensure the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by AI systems."[14] The Overlay is designed to provide security

[9] "Artificial Intelligence" National Institute of Standards and Technology, accessed March 2020, https://www.nist.gov/topics/artificial-intelligence

[10] ANSI INCITS 172-2002 (R2007) Information Technology – American National Standard Dictionary of Information Technology (ANSDIT)

[11] "Executive Order on Maintaining American Leadership in Artificial Intelligence" Executive Branch of the United States Government, February 2019 https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

[12] "Artificial Intelligence Using Standards to Mitigate Risk" Department of Homeland Security: Analytics Exchange Program, 2018 https://www.dhs.gov/sites/default/files/publications/2018_AEP_Artificial_Intelligence.pdf

[13]"U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools" National Institute for Standards of Technology, August 2018 https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

[14] "Draft Guidance for Regulation of Artificial Intelligence Applications" Office of Management and Budget, accessed June 2020 https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

controls that will aid HVA owners in addressing these risks presented by development and use of AI applications.

Cloud Computing

Although the concept of cloud computing has existed for decades, the widespread adoption in recent years has brought new organizational risks alongside the increased gains and efficiencies. NIST defines cloud computing as, “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”[15] Implementations vary between organizations, with some using it as an Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), or as is often the case, a combination of the three.

HVA system owners need to be acutely aware of how their organization implements cloud-based services and how information travels through the network and interacts with cloud services, as cloud-based services will require greater sophistication in systems governance and management. Although the interaction of cloud-based services and HVAs may not be as direct as sensitive data storage, issues such as software slowdown from a surge in the remote workforce nationwide can impact governance, coordination, and essential activities for maintaining the security of HVAs. Similarly, cloud-based services can introduce new attack vectors due to the distributed nature of cloud networks which could enable the spread of malware or attacks via a compromised device through previously unconnected systems or hardware.

NIST SP 800-144 identifies nine cloud-based cybersecurity risk areas: governance, compliance, trust, architecture, identity and access management, software isolation, data protection, availability, and incident response.[16] This document includes controls that address each of these nine areas and serve as a tool for agencies to use in securing their HVAs with respect to the cloud and cloud services.

Internet of Things

The full scope of technologies considered as part of Internet of Things (IoT) is not well defined but can be described as the set of devices that interacts with both the physical world and the digital world outside of the scope of normal information technology (IT) (e.g., a smartphone or computer). IoT includes some printers, thermostats, cars, televisions, cameras, locks, and even some refrigerators. Connecting these devices to the Internet can create new capabilities and increased efficiencies. IoT devices can also present unconventional cybersecurity risks; however, because these devices often do not have conventional IT interfaces or interactions within an organization.

As agencies incorporate IoT devices into their enterprise, HVA system owners should consider that IoT devices may enable adversaries direct/indirect access to an HVA. IoT devices may eventually provide mission essential functionalities to agencies; however, even if IoT devices do not rise to the level of mission essential, they should be inventoried and managed as potential attack vectors. National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 8228 identifies three cybersecurity and privacy risk considerations for IoT devices: the devices’ interaction with the physical world, their unconventional monitoring and management systems, and their pre-

[15] Peter Mell and Tim Grance “The NIST Definition of Cloud Computing”, September 2011, NIST SP 800-145 https://csrc.nist.gov/publications/detail/sp/800-145/final

[16] Jansen et. al., “Guidelines on Security and Privacy in Public Cloud Computing,” December 2011, NIST SP 800-144, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

market unconventional cybersecurity functionalities.[17] IoT devices are uniquely positioned because of their physical and logical interactions and interconnections. Adversaries may target these devices to sabotage device readings, attempt to exploit a more sensitive system through lateral movement of interconnected systems, or instigate a chain of events leading to an incident. These devices do not have conventional monitoring and management features which can prevent authorizing officials (AO) from managing and logging activity on these devices.

Similarly, IoT devices do not have conventional cybersecurity controls or management and may not have conventional cybersecurity requirements. Unmanned aerial systems or unmanned aerial vehicles (UAS/UAV) are examples of IoT-related devices that may have unique cybersecurity vulnerabilities that may still be translatable to more common ones. A study conducted on UAS/UAV cybersecurity vulnerabilities found that they may be subject to supply-chain vulnerabilities whereby suppliers install components that could maliciously alter the system's behavior. Attackers may also take advantage of unencrypted or poorly encrypted communication between the device and its controller, allowing the attackers indirect access to the device.[18] The Overlay offers controls that address these vulnerabilities and potentially others affecting UAS/UAVs. The Overlay generally serves as a tool to inform measures taken to secure HVAs as they pertain to UAS/UAVs and other IoT devices.

The Overlay also helps HVA system operators better manage the devices connected to their network and develop contingency plans in the event of their compromise. Finally, the Overlay offers an awareness and training control (AT-2 [1]) that, will help organizations create plans to train and create awareness for personnel that interact with IoT devices on a day-to-day basis.

HVA Control Overlay Summary

The control families and controls have been updated to reflect the final version of NIST SP 800-53 Rev 5. This version of the Overlay expands upon the FY18 Overlay with two control families that address supply chain risk management and PII protection training and awareness, risk assessments, configuration management, and others. The Overlay may be voluntarily implemented and is not mandatory; however, the Overlay's control families and controls address the latest threats and risks posed to HVAs as identified by the HVA PMO through analysis of existing HVA systems and assessment findings, trends, and the current, exigent cybersecurity threats known to CISA. Agencies are encouraged to adapt the Overlay, as needed, to their specific system operating environments and enterprise architectures.

In addition to the broader updates, the Overlay's individual controls have been adapted from NIST SP 800-53 Rev 5 and revised from the previous Overlay in the following ways:

- the 'Parameter Value' has been replaced with 'Control Direction,' which provides recommended guidance on how to implement the recommended control;
- the 'Discussion' has replaced the 'Supplemental Guidance' section for each control and offers additional context and suggestions for implementation, where applicable; and
- the 'Cybersecurity Framework (CSF) Function Mapping' that maps the control to the relevant

[17] Boeckl et. al, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," June 2019, NISTIR 8228,
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

[18] Kim et. al., "Cyber Attack Possibilities Analysis for Unmanned Aerial Vehicles," September 2012,
https://pdfs.semanticscholar.org/1a95/4775dd9a2596b7543af7693d707415077289.pdf

CSF Function, specifically Identify, Protect, Detect, Respond, and Recover.[19]

Figure 1 below provides a summary graphic of all NIST SP 800-53 Rev 5 security control families included in the Overlay.

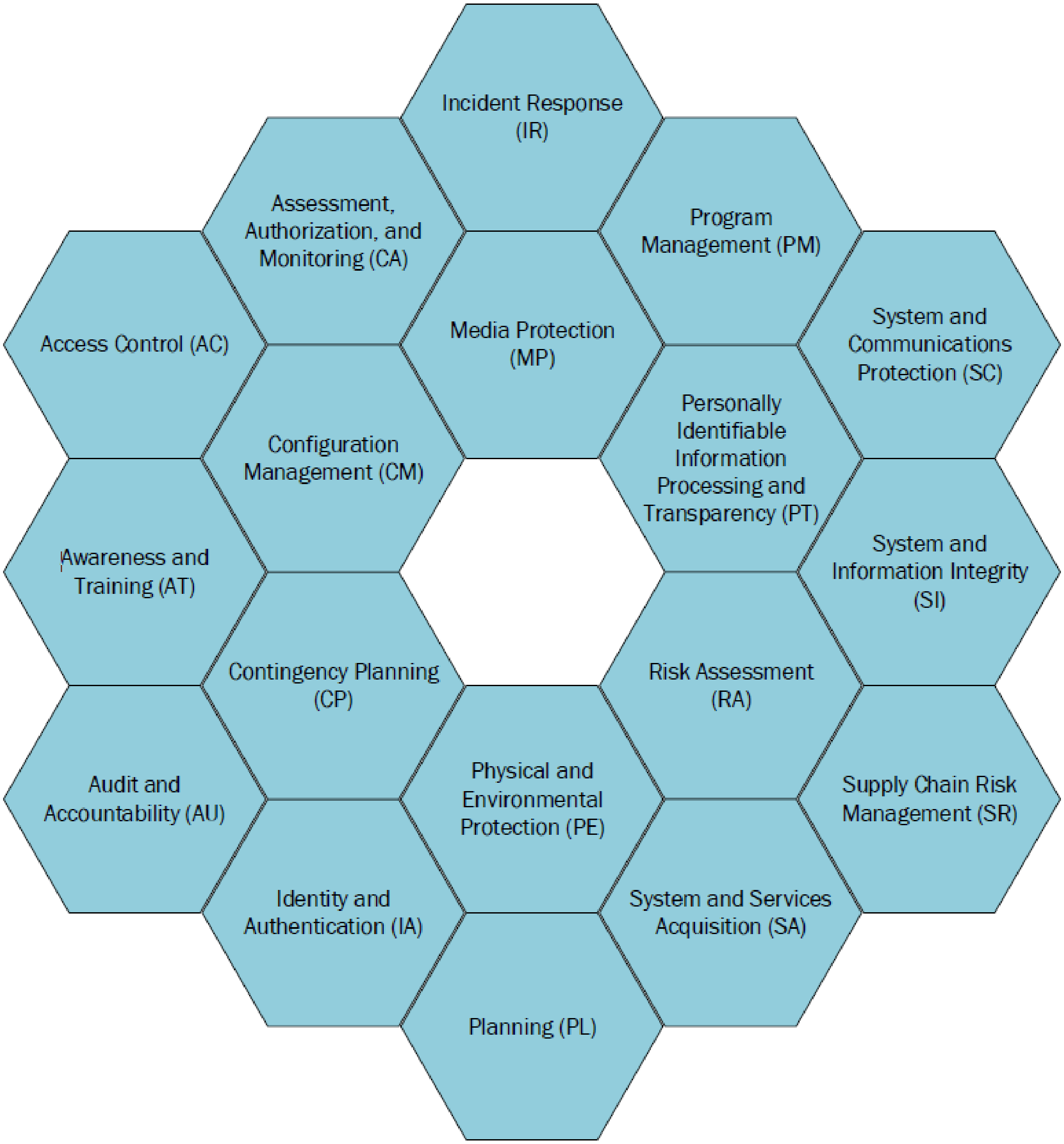

Incident Response (IR)
Assessment, Authorization, and Monitoring (CA)
Program Management (PM)
Access Control (AC)
Media Protection (MP)
System and Communications Protection (SC)
Configuration Management (CM)
Personally Identifiable Information Processing and Transparency (PT)
Awareness and Training (AT)
System and Information Integrity (SI)
Contingency Planning (CP)
Risk Assessment (RA)
Audit and Accountability (AU)
Physical and Environmental Protection (PE)
Supply Chain Risk Management (SR)
Identity and Authentication (IA)
System and Services Acquisition (SA)
Planning (PL)

Figure 1. HVA Control Overlay Security Control Families

[19] "Framework for Improving Critical Infrastructure Cybersecurity", NIST Cybersecurity Framework, April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

HVA Control Overlay Controls at a Glance

Table 1 below shows the number of controls and enhancements that comprise each control family within the Overlay. The number for each control family is representative of both HVA and enterprise-level controls and enhancements.

Control Family	Number of Controls and Enhancements
AC	12
AU	12
AT	1
CA	7
CM	8
CP	7
IA	7
IR	5
MP	2
PE	2
PL	4
PM	4
PT	2
RA	6
SA	8
SC	20
SI	13
SR	6

Table 1. Controls and Enhancements by Control Family

Using the HVA Control Overlay

HVA PMO recommends organizations implement the listed base controls and enhancements in the 'High Value Asset Controls' and 'Enterprise Controls' sections below. HVA controls are intended to be implemented at the HVA system/component level and enterprise controls should be implemented at the enterprise level to secure the enterprise systems, architectures and networks that support HVA operations.

Table 2 provides an example of a control table found within this section. Each control table generally describes why HVA PMO recommends selecting the control, as well as implementation guidance, references, and CSF function mapping. Detailed explanations of each field within the control tables in the Overlay are listed in the example control table 2.

The HVA PMO selected the Overlay's controls and enhancements based on the results of HVA assessments conducted by CISA, combined with up-to-date threat intelligence and cybersecurity trends. The Overlay is not a compliance-based document but offers controls and enhancements designed to address the assessment finding trends and risks relevant to HVAs. The Overlay includes only those controls that fall within the scope of these criteria and does not exhaustively list base controls (or enhancements) for each family. In instances that an enhancement is listed in the Overlay but not the associated base control, the HVA PMO still recommends that organizations implement the base control. NIST SP 800-53 Rev 5 also states that control enhancements are intended to be implemented in conjunction with the related base control. In accordance with this guidance, the HVA

PMO recommends organizations endeavor to implement the base controls associated with the enhancements listed in the Overlay, prior to implementing the enhancement.

Table 2 below is for example purposes only and should not be implemented on any HVA. Implementation of this control may introduce unacceptable risk to the HVA.

<table>
<tr><th colspan="2">AC-2 (9) ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS</th></tr>
<tr><td>Control Selection Rationale</td><td>The control selection rationale indicates the reason for selecting the control for an HVA and specifies the risk(s) that the control addresses.</td></tr>
<tr><td>Control Direction:</td><td>The control direction provides recommended guidance on how the control should be implemented on an HVA or HVA component. The control direction may be comprised of multiple items, which will be indicated by one or more item identifiers listed under the ‘Control Direction’ title.</td></tr>
<tr><td>Discussion</td><td>Provides additional context and implementation suggestions for the control, where applicable.</td></tr>
<tr><td>Related Controls</td><td>Lists the NIST SP 800-53 Rev 5 control(s) that are related to the specific control identified in the control table.</td></tr>
<tr><td>References</td><td>Provides references that are related to the control and those that may be leveraged for additional information regarding the control.</td></tr>
<tr><td>CSF Function Mapping</td><td>Maps the control to the relevant CSF function (identify, detect, protect, respond, and/or recover). Controls may map to one or more CSF function.</td></tr>
</table>

Table 2. Unsuitable Security Controls for HVAs

High Value Asset Controls

This section provides details on the security controls as they apply to the Overlay. The controls in this section expand on or adapt those contained in NIST SP 800-53 Rev 5 and may have additional control specifications not present in the NIST SP 800-53 Rev 5 and vice versa. The controls in this section are generally recommended to be implemented at the HVA system level and may not be appropriate or as effective if applied across the enterprise.[20] The Overlay offers specific controls and implementation guidance to address risks facing federal HVAs. As such, the Overlay may not list the base control associated with a given enhancement and does not provide an exhaustive list of all controls contained within NIST SP 800-53 Rev 5.

NIST SP 800-53 Rev 5 also states that control enhancements are intended to be implemented in conjunction with the related base control. In accordance with this guidance, the HVA PMO recommends organizations endeavor to implement the base controls associated with the enhancements listed in the Overlay, prior to implementing the enhancement.

Access Control (AC)

AC-2 ACCOUNT MANAGEMENT		
Control Selection Rationale		User and system account management is critical in establishing an effective access control framework for the environment and HVA. The access control framework provides the mechanisms to control and limit access to individuals who have a need to access the HVA information and systems.
Control Direction:		The organization should:
	Item e	require approvals by at least two appropriate organizational personnel (e.g., system owner, mission/business owner, Authorizing Official, Chief Information Security Officer [CISO], etc.) for requests to create system accounts;
	Item h	notify appropriate organization personnel within 12 hours when temporary accounts or privileged accounts are no longer required, users are terminated or transferred, and upon user’s need-to-know changes;
	Item j	review privileged accounts, at least quarterly, for compliance with account management requirements. Privileged account access should be re-authorized for the HVA at least annually. Review user accounts, at least, annually for compliance with account management requirements; and
	Item m	prohibit creating and using guest, anonymous, and shared HVA accounts (including shared administrator and root accounts) for access to all information types processed by the system. NOTE: Anonymous is allowed for read-only, public-facing information websites.

[20] Organizations are not required to implement all of the Overlay’s controls for each HVA component.

Discussion	Examples of HVA account types include individual, system, guest, emergency, developer, temporary, and service. Identification of authorized HVA users and the specification of access privileges reflects the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. External system accounts are not included in the scope of this control. Organizations should address external system accounts through organizational policy.
Related Controls	AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, SC-7, SC-13, SC-37.
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

AC-2 (2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

Control Selection Rationale	Temporary and Emergency HVA accounts are considered high-risk because they often do not have multifactor authentication. These types of accounts are tightly controlled, monitored, and removed promptly when no longer required to avoid unauthorized access to the HVA.
Control Direction:	The organization should automatically disable temporary and emergency accounts within 12 hours of issuance.
Discussion	Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time-period, rather than at the convenience of the systems administrator. Automatic removal or disabling of accounts provides a more consistent implementation.
Related Controls	N/A
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

AC-3 ACCESS ENFORCEMENT

Control Selection Rationale	The system enforces approved access authorizations to the system and information to ensure protection against unauthorized access. The systems limit user access to information according to defined access policies to ensure the security and confidentiality of the information.
Control Direction:	The organization should control access to the HVA and HVA information in accordance with the principle of least privilege through automated access enforcement solutions such as mandatory access control (MAC) as with AC-3(3), discretionary access control (DAC) as with AC-3(4), role-based access control (RBAC) as with AC-3(7), or attribute-based access control (ABAC) as with AC-3(13). This automated access enforcement is limited, to the maximum extent possible, so that each entity (user, privileged, and service accounts) has access to only the pieces of information necessary for their job and in accordance with their approved access authorization. Access enforcement must reside in the HVA environment and not on another system (i.e., cannot be inherited).
Discussion	Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational HVAs. In addition to enforcing authorized access at the HVA system level and recognizing that systems can host many applications and services in support of missions and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.
Related Controls	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, SA-17, SC-2, SC-3, SC-4, SC-13, SC-28, SC-31, SC-34, SI-4
References	OMB Circular A-130
CSF Function Mapping	Protect

AC-3 (9) ACCESS ENFORCEMENT | CONTROLLED RELEASE	
Control Selection Rationale	The HVA can only protect organizational information within the confines of established system boundaries. Additional security controls may be needed to ensure that such information is adequately protected once it is passed beyond the established HVA boundaries. HVA information shared or exchanged outside the authorization boundary may be at increased risk of unauthorized access and use.
Control Direction:	The organization should implement controlled release such that the external system provides a level of protection commensurate with the confidentiality, integrity, and availability impact levels of the information being shared
Discussion	In situations where the HVA is unable to determine the adequacy of the protections provided by external entities, as a mitigating control, organizations should determine procedurally whether the external systems are providing adequate controls. The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received does not need to be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals' privacy. The external entity should provide a copy of the authorization to operate for the system that will process, store, or transmit the HVA information. The ATO should be current and signed.
Related Controls	CA-3, PT-2, PT-3, PT-8, SA-9, SC-16
References	OMB Circular A-130
CSF Function Mapping	Protect

AC-4 INFORMATION FLOW ENFORCEMENT	
Control Selection Rationale	Enforcing and controlling the flow of information inside and transiting the HVA authorization boundary ensures that the information and mission-critical services are protected at a level commensurate with the risk to the system and information.
Control Direction:	The organization should enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. Flow control is point to point, protocol and port specific and protects confidentiality and integrity of information on networks at a lower protection level than the information being transmitted. (e.g., PII on Internet). Enforcement of information flow is controlled at the authorization boundary using boundary protection

	devices (e.g., gateway, router, guard, encrypted tunnel, firewall, application proxy etc.) or at tiered points within the authorization boundary.
Discussion	Information flow control regulates where information can travel within a system and between systems (in contrast to who may access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces risk that such transfers violate one or more domain security or privacy policies.
Related Controls	AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

AC-5 SEPARATION OF DUTIES

Control Selection Rationale	The organization can reduce the risk of abuse of authorized HVA access/use privileges and malevolent activity without collusion through separation of duties.
Control Direction:	The organization should:
Item a	establish and document organization-defined roles and duties for the individuals that require separation; and
Item b	define HVA system access authorizations to support separation of duties as established in ‘Item a’ above.
Discussion	Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations should consider the entirety of systems and system components when developing policy on separation of duties. This control is enforced through the account management activities in AC-2 and access control mechanisms in AC-

	3. Separation of duties supports HVA or HVA system component testing in control CM-4.
Related Controls	AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-5, MA-3, MA-5, PS-2, SA-8, SA-17
References	CM-4
CSF Function Mapping	Protect

AC-6 LEAST PRIVILEGE	
Control Selection Rationale	Organizations can protect the information and mission critical services at a level commensurate with the risk to the HVA and information by granting only the necessary rights to support the mission and business function.
Control Direction:	The organization should control and limit access for HVA users in accordance with the principle of least privilege.
Discussion	Organizations should employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations should consider the creation of additional processes, roles, and accounts as necessary, to achieve least privilege. Organizations should apply least privilege to the development, implementation, and operation of organizational systems.
Related Controls	AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38
References	OMB Circular A-130
CSF Function Mapping	Protect

AC-6 (5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	
Control Selection Rationale	The organization can protect privileged accounts from unauthorized access or loss of integrity by protecting them at a higher level than non-privileged accounts. Privileged accounts are targeted by adversaries because of the elevated rights granted to those accounts.
Control Direction:	The organization should restrict and limit privileged accounts rights to only those functions, services, and attributes necessary to perform the required task(s).

Discussion	Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off the shelf (COTS) operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided they retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.
Related Controls	IA-2, MA-3, MA-4
References	OMB Circular A-130
CSF Function Mapping	Protect

AC-6 (7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES	
Control Selection Rationale	The organization can, through periodic HVA-associated account reviews, verify user access permissions are still relevant and necessary to ensure that they cannot be leveraged for unauthorized access.
Control Direction:	The organization should annually review the rights assigned to user accounts and validate the need for such rights, as well as conduct quarterly reviews of the rights assigned to privileged accounts and validate the need for such privileges.
Discussion	The need for certain assigned user privileges may change over time reflecting changes in organizational missions and business functions, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations should take appropriate corrective actions. HVA account reviews may be conducted on a more frequent basis due to the sensitivity of the HVA system and information.
Related Controls	CA-7
References	OMB Circular A-130
CSF Function Mapping	Protect

AC-17 REMOTE ACCESS	
Control Selection Rationale	The organization can protect the HVA information, integrity of the controls implemented, and operating in the environment by controlling and limiting access to the HVA environment from remote locations (outside the HVA authorization boundary).
Control Direction:	The organization should limit remote access to the HVA environment from locations outside of the HVA authorization boundary.
Discussion	Remote access is access to organizational systems (or processes acting on behalf of users) communicating through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. Remote access into the HVA environment is restricted and controlled at the authorization boundary of the HVA. Entities that leverage enterprise remote access solutions from systems outside the enterprise must further control access at the HVA authorization boundary into the HVA environment over the support systems' network. Likewise, systems outside the HVA authorization boundary but located on a support system's authorization boundary are considered remote access devices to the HVA and must be controlled and limited when accessing the HVA environment.
Related Controls	AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SI-4
References	OMB Circular A-130, NIST SP 800-46, NIST SP 800-77, NIST SP 800-113
CSF Function Mapping	Protect

AC-17 (2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION	
Control Selection Rationale	The organization can protect HVA information from unauthorized access in transit by using encryption capabilities for HVA remote access data/sessions.
Control Direction:	The organization should implement encryption capabilities to protect the confidentiality and integrity of HVA remote access sessions.
Discussion	Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet

	communications and online transactions.
Related Controls	SC-8, SC-12, SC-13
References	OMB Circular A-130
CSF Function Mapping	Protect

AC-20 USE OF EXTERNAL SYSTEMS

Control Selection Rationale	The organization can implement terms and conditions consistent with security and privacy requirements for the HVA and HVA information to reduce the risk of loss of confidentiality or integrity when accessing or processing HVA information on external systems or environments.
Control Direction:	The organization should establish detailed terms and conditions of acceptable use, in accordance with organizational security policies and procedures and federal guidelines and laws. These terms and conditions (contractual requirements for vendors/consultants) should specify types of access allowed into the environment, security requirements for the external system, information handling limitations and restrictions. This control does not extend to external systems used to access public information that does not need protecting.
Discussion	External systems are systems that are used by, but not a part of, organizational systems and for which the organization has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness.
Related Controls	AC-2, AC-3, AC-17, CA-3, PL-2, SA-9, SC-7
References	OMB Circular A-130, Federal Information Processing Standards (FIPS) 199
CSF Function Mapping	Identify, Protect

Awareness and Training (AT)

AT-2 (1) AWARENESS TRAINING | PRACTICAL EXERCISES

Control Selection Rationale	The organization can reduce the number of successful intrusions or attacks (such as phishing and spear phishing attacks or threat actors gaining unauthorized access to or obtaining data) through practical exercises in awareness training that simulate events and incidents.
Control Direction:	The organization should implement a cybersecurity user awareness and training program for HVA system owners and operators that includes practical exercises. The organization should administer practical exercises to the HVA owner/operator:

Item a	prior to first use of the HVA;
Item b	after a significant change to the HVA such that the prior exercises no longer reflect the risks and functions of the current HVA; and
Item c	when exercises, training courses or requirements are updated.
Discussion	Practical Exercises may include, for example, simulated counterfeit detection, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, or malicious weblinks. Training may be regularly updated to reflect the most current, exigent cybersecurity threats posed to the HVA or the organization. Organizations may also update the minimum training requirements to operate the HVA, which may require the HVA owner or operator to complete the new training.
Related Controls	CA-2, CA-7, CP-4, IR-3
References	OMB Circular A-130, NIST SP 800-50, NIST SP 800-160 v2
CSF Function Mapping	Protect

Audit and Accountability (AU)

AU-2 EVENT LOGGING	
Control Selection Rationale	Auditing of specific events allows for the detection, tracing, and tracking of users and processes actions used to identify potential threats and attacks against the HVA information and systems.
Control Direction:	The organization should:
Item a	audit successful and failed logins (Operating System [OS] and data repositories), audit success and failed computer account activities (OS and data repositories), audit success and failed account and user management activities (OS and data repositories), unsuccessful attempts to access database, enterprise synchronized date, time, and time zone for each event, source Internet Protocol (IP), port and protocol, destination IP, port and protocol, and others.
Discussion	The parameter value (item a) identified is not an exhaustive list of all auditable events but identifies the minimum specific events to be audited for HVAs. Organizations determine what, if any, additional events are to be audited based on a risk assessment.
Related Controls	AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-8, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11
References	OMB Circular A-130, United States Computer Emergency Readiness

	Team (US-CERT) “Federal Incident Reporting Guidelines,” NIST SP 800-92
CSF Function Mapping	Identify

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Control Selection Rationale	Increased frequency analysis of HVA system logs and events is necessary to detect and report potential incidents or breaches of HVA information, loss of integrity, or loss of availability.
Control Direction:	The organization should:
Item a	review, analyze, and alert on system audit records in cyber-relevant time[21] for indications of inappropriate, unusual activity (e.g., concurrent logons), breaches, or threats; and
Item b	report incidents and findings in accordance with US-CERT reporting timeframes and requirements.
Discussion	Given the sensitivity of the information and systems, the analysis of the logs and events are performed more frequently and with more rigor than non-HVA systems. Reporting of potential incidents comply with US-CERT requirements. Cyber-relevant time is the relative speed at which an adversary is attacking a network, application, system, or other resource.
Related Controls	AC-2, AC-3, AC-6, AC-17, AU-16, CA-7, CM-6, IA-2, IA-3, IA-5, IA-8, PE-3, RA-5, SC-7, SC-18, SI-3, SI-4
References	OMB Circular A-130, US-CERT “Federal Incident Reporting Guidelines,” NIST SP 800-92
CSF Function Mapping	Detect, Respond

AU-9 PROTECTION OF AUDIT INFORMATION

Control Selection Rationale	The organization can protect audit information by protecting it at the same level as the HVA that generated the audit information. This will help to ensure that any potential HVA information contained within audit logs is protected adequately.
Control Direction:	The organization should:
Item a	

[21] Herring, MJ, and KD Willett. “Active Cyber Defense: A Vision for Real-Time Cyber Defense.” *Journal of Information Warfare*, vol. 13, no. 2, 2014, pp. 46–55. *JSTOR*, www.jstor.org/stable/26487121. Accessed 14 Dec. 2020.

	protect audit information to the highest level commensurate with the highest security protection level of the information contained within the audit events.
Discussion	Audit information includes all information, for example, audit records, audit log settings, audit reports, and personally identifiable information, needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.
Related Controls	AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4
References	OMB Circular A-130, NIST SP 800-92
CSF Function Mapping	Protect

AU-9 (2) PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS

Control Selection Rationale	Protecting audit information integrity on the HVA is critical for accurate and timely incident response management and accountability.
Control Direction:	The organization should protect system audit information by storing/transferring audit information to a physically different system from the system that generated the events.
Discussion	Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.
Related Controls	AU-4, AU-5
References	OMB Circular A-130, NIST SP 800-92
CSF Function Mapping	Protect

AU-9 (3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION	
Control Selection Rationale	Protecting audit information integrity on the HVA is necessary for accurate accountability and traceability of HVA actions.
Control Direction:	The organization should implement cryptographic solutions (e.g., hashing function) to protect the integrity of audit information at rest.
Discussion	Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.
Related Controls	AU-10, SC-12, SC-13
References	OMB Circular A-130
CSF Function Mapping	Protect

AU-9 (5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION	
Control Selection Rationale	Protecting audit log management is critical for maintaining the integrity of logs and accountability of user actions.
Control Direction:	The organization should enforce dual authorization (two appropriate personnel such as system owner, mission/business owner, AO, CISO, etc.) for manual movement and deletion of system audit logs.
Discussion	To protect the integrity and availability of audit information organizations control access and authorizations of privileged users to modify and delete audit logs. Logs are retained in accordance with federal, department, and agency requirements. After the retention requirement period organizations may have a need to delete or move audit information from systems. Dual authorization approvals by at least two appropriate personnel (system owner, mission/business owner, AO, CISO, etc.) is required for movement or deletion of audit files. Automated systems can be configured to automatically archive or remove audit logs according to policy.
Related Controls	AC-3
References	OMB Circular A-130
CSF Function Mapping	Protect

AU-9 (6) PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS

Control Selection Rationale	Protection of audit integrity through read-only access limits the potential that users can delete or modify critical audit files.
Control Direction:	The organization should ensure that access to audit logs are read-only for authorized individuals (privileged accounts only).
Discussion	Only limited privilege accounts with the need to know have read-only access to audit logs. All other users do not have any access to HVA logs. Organizations limit and restrict any accounts, in accordance with AU-9(5), with access to write or delete audit logs.
Related Controls	AU-9(5)
References	OMB Circular A-130
CSF Function Mapping	Protect

AU-10 NON-REPUDIATION

Control Selection Rationale	Non-repudiation is necessary to ensure accountability for correlating system actions with users or system accounts in the system event logs.
Control Direction:	The organization should implement HVA non-repudiation for users, privileged users, system accounts, and service accounts. All accounts, include system and service accounts, are traceable back to an accountable individual
Discussion	Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, or approving a procurement request, or received specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.
Related Controls	AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23
References	OMB Circular A-130
CSF Function Mapping	Identify

AU-16 CROSS-ORGANIZATIONAL AUDIT LOGGING	
Control Selection Rationale	External systems and services to support the HVA maintain auditing capabilities, non-repudiation of the users, and correlation of actions across the external systems allows for accurate and timely organizational incident response capabilities.
Control Direction:	The organization should require that the contractor or external hosting entity comply with federal and agency audit requirements in the external environments.
Discussion	The external system provides non-repudiation for non-public user access to HVA information for accountability.
Related Controls	AU-3, AU-6, AU-7, CA-3, PT-8
References	OMB Circular A-130, NIST SP 800-150
CSF Function Mapping	Identify

Assessment, Authorization, and Monitoring (CA)

CA-3 INFORMATION EXCHANGE	
Control Selection Rationale	The organization can minimize, protect, and control HVA information exchange with external entities through Interconnection Security Agreements (ISAs) and Memorandum of Understanding/Agreements (MOU/As) to protect confidentiality, integrity, and availability of the information.
Control Direction:	The organization should:
Item c	review and update ISAs and MOU/As at least annually and in response to environmental or operational changes to either system.
Discussion	Organizations should create, authorize, and track ISA documents for each external support services and each external connection (outside the authorization boundary) to and from the HVA. In the case of external connections, the ISA includes technical details to include but not limited to: IP addresses, Doman Name System (DNS) names, protocols, ports, frequency of transfers, incident response contacts at both organizations, description of data exchanged, direction of data exchange, sensitive level of data exchanged, security categorization of both systems, and ATO status. For external support services the ISA minimally includes service description, expected availability (uptime) of the service, technical point of contacts, incident response contacts at both organizations, importance of the external service, security categorization of both systems, and ATO status.

	The organization should develop and implement a MOU/A or Business Associate Agreement that describes the acceptable uses of the information exchanged, restrictions on sharing the information, and at what level the information is to be protected. Any proposed environmental or operational changes are communicated to both parties and a risk assessment is performed to determine the impact to both organizations due to the change prior to implementation. Reduction of the data set exchanged to the minimum data elements necessary for the receiving organization to perform their function should be considered. A risk assessment is performed on the reduced data elements to determine if the information impact level has changed.
Related Controls	AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-8, RA-3, SA-9, SC-7, SI-12
References	OMB Circular A-130, FIPS 199, NIST SP 800-47
CSF Function Mapping	Identify, Detect

CA-5 PLAN OF ACTION AND MILESTONES	
Control Selection Rationale	The organization can track and monitor remediation progress for the HVA and supporting systems through plans of action and milestones (POA&M). Tracking and monitoring remediations for supporting systems from which the HVA inherits controls is necessary to ensure that the HVA is not unknowingly accepting risk from the control interdependencies.
Control Direction:	The organization should:
Item b	review and update the HVA systems and supporting system's POA&M at least monthly, and ensure it is signed off by the AOs [dual AOs - see AU-9 (5)] at least quarterly.
Discussion	HVA systems are to be prioritized for timely remediation of weaknesses and deficiencies to minimize the risks to the HVA. Organizations should prioritize remediation efforts based on the risk to the systems to remediate highest risks first. Prioritized POA&M management informs the planning, programming, budgeting and execution (PPBE) cycles associated with remediation and/or aligned with development modernization enhancement (DME) projects. agencies ensure that adequate and timely resources are allocated to support remediation efforts. All supporting system weaknesses and deficiencies are tracked and reviewed by HVA Authorizing Officials to ensure systems risks are remediated expeditiously.
Related Controls	CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12
References	OMB Circular A-130, NIST SP 800-47
CSF Function Mapping	Identify, Detect, Protect

CA-6 AUTHORIZATION	
Control Selection Rationale	Authorizations are the official ATO for HVA systems and are issued by the AO where the formal acceptance of the risk to organizational operations and assets, people, interconnections, and the Nation is recorded.
Control Direction:	The organization should:
Item a	assign a senior official as the authorizing official for the HVA;
Item b	assign a senior official as the authorizing official for common controls available for inheritance by organizational HVAs;
Item c	ensure that the authorizing official for the HVA, before commencing operations: accepts the use of common controls inherited by the HVA and authorizes the HVA to operate;
Item d	ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; and
Item e	update the HVA authorization at the end of the 3-year authorization window, or as needed.
Discussion	The AO must completely understand the risks, to the organization and Nation, of operating the HVA. The Security Control Assessment process is inclusive of all identified risks from systems, components, information, interconnections, users, vulnerabilities, and threats. If the Security Control Assessment results in a pre-determined unacceptable level of residual risk to the system, the organization should remediate issues to reduce the risk to an acceptable level or rescinds the HVAs ATO. Omitting information from the Security Control Assessment could result in this decision process being conducted with inaccurate or incomplete information leading to the HVA operating in an unknown risk state.
Related Controls	CA-2, CA-3, CA-7, PM-9, PM-10, SA-10, SI-12
References	OMB Circular A-130, NIST SP 800-37, NIST SP 800-137
CSF Function Mapping	Identify

CA-6 (1) AUTHORIZATION | JOINT AUTHORIZATION – INTRA-ORGANIZATION	
Control Selection Rationale	Assigning multiple AOs from the same organization to serve as co-AOs for the HVA increases the transparency of the HVA operating risks and decreases the level of subjectivity in the risk-based decision-making

	process for security and privacy.
Control Direction:	The organization should employ a joint authorization process for the HVA that includes multiple AOs from the same organization conducting the authorization.
Discussion	The HVA authorization process represents all HVA dependent functions/missions in the authorization process to ensure that risk-based decisions are transparent and reflective of the risk-tolerance of all missions that are reliant on the HVA. The joint authorization process makes it clear that co-AOs are equally responsible for authorizing and accepting risks to the HVA system. All system documentation that is typically required to be signed by the AO is to be signed by both co-AOs for this system.
Related Controls	AC-6
References	OMB Circular A-130, NIST SP 800-37, NIST SP 800-137
CSF Function Mapping	Identify

CA-7 CONTINUOUS MONITORING

Control Selection Rationale	An HVA continuous monitoring strategy promotes timely risk awareness and remediation as risks change in cyber-relevant time.
Control Direction:	The organization should develop an HVA system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level information security continuous monitoring (ISCM) strategy.
Discussion	Continuous Monitoring provides continuous assurance that security controls are effectively meeting organizational protection needs. Organizations should develop a continuous monitoring strategy in accordance with NIST SP 800-137 "ISCM" to include all selected security controls in use for the systems. The ISCM strategy is maintained to address information security risks and requirements across the organizational risk management tiers. The ISCM strategy is implemented and updated, in accordance with an organization-defined frequency, to reflect the effectiveness of deployed controls, significant changes to information systems, and adherence to federal statutes, policies, directives, instructions, regulations, standards, and guidelines. Use of automated tools and mechanisms is prioritized where possible. Continuous Monitoring programs follow federal guidance and reporting requirements per OMB Circular A-130 "*Managing Information as a Strategic Resource*" and comply with Continuous Diagnostics and Mitigation (CDM) reporting requirements. External service providers hosting HVA information and mission critical services are required to meet federal, CISA CDM, and organizational ISCM requirements. The

	organization should leverage ISCM capabilities to support the migration to the ongoing authorization (OA) process.
Related Controls	AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-8, RA-3, RA-5, RA-7, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SC-38, SI-3, SI-4, SI-12, SR-6
References	OMB Circular A-130, NIST SP 800-37, NIST SP 800-137
CSF Function Mapping	Detect, Protect, Respond

CA-7 (3) CONTINUOUS MONITORING | TREND ANALYSIS

Control Selection Rationale	Threats change over time and may increase the risk to the HVA. These changes can drive the frequency and rigor of continuous monitoring activities performed on the HVA and can reveal patterns of behavior, behavioral anomalies, fraud, and other Indicators of Compromise (IOCs) that require the risk posture of the HVA to be reviewed.
Control Direction:	The organization should employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.
Discussion	Trend analyses include examining recent threat information addressing the types of threat events that have occurred within the organization or the Federal Government; success rates of certain types of attacks; emerging vulnerabilities in technologies; evolving social engineering techniques; the effectiveness of configuration settings; results from multiple control assessments; and findings from Inspectors General or auditors.
Related Controls	N/A
References	OMB Circular A-130, NIST SP 800-37, NIST SP 800-137, US-CERT Technical Cyber Security Alerts
CSF Function Mapping	Identify, Protect

CA-9 INTERNAL SYSTEM CONNECTIONS

Control Selection Rationale	Authorizing internal connections to and from the HVA within its boundaries can mitigate risks posed to the HVA system and information due to potential compromise of the connected components.
Control Direction:	The organization should:

Item a	document and authorize internal connections between the HVA environment and other organizational systems (including support systems). Organizations may choose to develop a streamlined version of a typical ISA/MOU to be used for internal connections.
Discussion	Organizations should identify the connections between the HVA and other system components within the HVA boundary to understand the critical dependencies of the HVA. In conjunction with CA-6(1), the Overlay specifies that these interconnections are to be documented and authorized in accordance with the Joint Authorization methodology.
Related Controls	AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12
References	OMB Circular A-130, OMB M-19-03
CSF Function Mapping	Protect

Configuration Management (CM)

CM-2 BASELINE CONFIGURATION	
Control Selection Rationale	The organization can use the established baseline configuration of an HVA to determine if deviations or changes to the configuration have occurred. The baseline can be used as the basis for future configurations and allow the organization to restore the HVA to previous settings, if required.
Control Direction:	The organization should:
Item a	develop, document, and maintain a current baseline configuration of the HVA; and
Item b	review and update the baseline configuration of the HVA at least annually, when required due to updates to the HVA software or operating system, and when system components are installed or upgraded.
Discussion	Baseline configurations for the HVA and HVA components include connectivity, operational, and communications aspects. Baseline configurations are documented, formally reviewed and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines

	as organizational systems change over time. Baseline configurations of the HVA may or may not reflect the current enterprise architecture (EA), depending on the nature of the HVA and its function(s) (i.e. mainframe-based HVAs or other legacy and/or specialized system).
Related Controls	AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18
References	NIST SP 800-124, NIST SP 800-128
CSF Function Mapping	Protect, Detect

CM-3 (2) CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES

Control Selection Rationale	The organization can minimize the negative impacts and unintended effects of changes to the HVA by testing, validating, and documenting the intended changes to the HVA.
Control Direction:	The organization should test, validate, and document configuration changes to the HVA before finalizing and implementing the changes.
Discussion	Changes to the HVA include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations should ensure testing does not interfere with HVA operations supporting organizational missions and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, HVA security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. An operational HVA may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If the HVA must be taken off-line for testing, the tests should be scheduled to occur during planned system outages, when possible. If the testing cannot be conducted on an operational HVA, organizations should annotate an acceptance of risk in the HVA system security plan and/or consider employing compensating controls, such as CM-2 and CM-3(7).
Related Controls	N/A
References	CM-6, NIST SP 800-124, NIST SP 800-128, NISTIR 8062
CSF Function Mapping	Protect, Detect

CM-3 (7) CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES

Control Selection Rationale	The organization can reduce the risks posed by unauthorized changes to the HVA by regularly reviewing configuration changes to the HVA.
Control Direction:	The organization should review changes to the HVA at least twice a year or when dictated by the organization's configuration change control process to determine whether unauthorized changes have occurred.
Discussion	Indications that warrant review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process.
Related Controls	AU-6, AU-7, CM-3
References	N/A
CSF Function Mapping	Protect, Detect

CM-4 (1) IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS

Control Selection Rationale	Organizations can analyze HVAs in a separate test environment for flaws, weaknesses, incompatibilities, or intentional alterations. Separate test environments reduce the risk of security and privacy impacts stemming from a change (such as software or hardware-based) to the HVA before it is introduced to the operational or production environment.
Control Direction:	The organization should analyze proposed changes to the HVA in a separate testing environment prior to implementing the changes in the organization's operational or production environment.
Discussion	A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments cannot be implemented, organizations should determine the strength of the mechanism required when implementing logical separation. HVA system owner and HVA system component tester roles and duties should be separate, as outlined in control AC-5. Appropriate separation of duties supports valid testing of the HVA, helps to protect the integrity of the HVA, and reduces potential conflicts of interest between testers, operators, developers, or individuals that directly interact with the HVA or its components prior to production environment implementation.
Related Controls	SA-11, SC-7

CM-4 (1) IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS	
References	AC-5, NIST SP 800-128
CSF Function Mapping	Protect

CM-6 CONFIGURATION SETTINGS	
Control Selection Rationale	Developing and tracking HVA baseline configurations help to establish common configurations for the HVA and allow for better detection of unauthorized modification or changes which could indicate a compromise of information and mission critical services.
Control Direction:	The organization should establish and document baseline configuration settings for HVA components and track deviations from established baselines for the HVA and components that comprise the HVA and:
Item a	ensure the HVA baseline configurations enforce secure authentication;
Item b	ensure the HVA does not allow for a common local administrator password on all the workstations, servers, and systems;
Item c	ensure default configurations and passwords of HVA commercial and government-off-the-shelf (COTS/GOTS) products are modified and not left as default;
Item d	verify the default configurations are not reverted to each time the HVA COTS packages are updated or upgraded; and
Discussion	Configuration settings apply to HVA systems and the HVA components. Changes to those configuration settings are monitored, tracked, and controlled by the organization.
Related Controls	AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

CM-6 (2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES

Control Selection Rationale	Responding to unauthorized changes on a system in a timely manner and structured approach reduces the likelihood of the loss of information or system functionality.
Control Direction:	The organization should respond to unauthorized changes to documented and authorized HVA configurations in accordance with the organizational configuration management policies and procedures.
Discussion	Organizations should cross reference detected changes with change control documentation to determine if the change was preauthorized. Organizations should be prepared for action and ensure processes are documented on detection of unauthorized changes to systems. Organizations should also employ safeguards to respond to and remediate unauthorized changes to configuration settings. All unauthorized changes are to be reported in accordance with the organization’s incident response processes.
Related Controls	IR-4, IR-6, SI-7
References	OMB Circular A-130
CSF Function Mapping	Detect, Respond

CM-7 (1) LEAST FUNCTIONALITY | PERIODIC REVIEW

Control Selection Rationale	Organizations can identify, disable and remove unnecessary HVA functions and services by periodically reviewing the functions, ports, protocols, and services utilized by the HVA or its component(s). Organizations can reduce the attack surface threat actors can use to directly or indirectly gain access to the HVA.
Control Direction:	The organization should:
Item a	review the HVA configuration at least quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services; and
Item b	take steps to disable unnecessary and/or non-secure functions, ports, protocols, and services that do not hinder or otherwise impede the organization’s ability to complete its mission essential function(s), as performed by the HVA.
Discussion	Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IP version [v] 4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can decide on the relative security of the function, port, protocol,

	and/or service or base the security decision on the results of periodic reviews of other organizations. Unsecure protocols include Bluetooth, file transfer protocol, and peer-to-peer networking.
Related Controls	AC-18
References	FIPS Publication 140-3, FIPS 180-4, FIPS 186-4, FIPS 202, NIST SP 800-167
CSF Function Mapping	Protect

CM-8 SYSTEM COMPONENT INVENTORY	
Control Selection Rationale	Establishing and maintaining a complete and accurate inventory of all system components within the HVA authorization boundary is crucial in ensuring that all risks to the HVA are characterized and addressed.
Control Direction:	The organization should:
Item b	review and update the HVA system device inventory at least every 72 hours consistent with CISA CDM reporting requirements, where applicable.
Discussion	Organizations may implement automated solutions to perform component inventory of the environment within the CISA CDM requirement timeframe.
Related Controls	CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PM-5, SA-4, SA-5, SI-2, SR-4
References	OMB Circular A-130, CISA CDM Reporting Requirements
CSF Function Mapping	Identify, Protect, Detect

Contingency Planning (CP)

CP-4 CONTINGENCY PLAN TESTING	
Control Selection Rationale	HVA contingency plan testing is important for organizations to determine the effectiveness of the contingency plan and identify areas for improvement.
Control Direction:	The organization should
Item a	fully test the HVA contingency plan on an annual basis plan to determine the effectiveness of the plan, identify weaknesses in the plan and readiness to execute the plan;
Item b	review the HVA contingency plan testing results; and

Item c	initiate corrective actions to the HVA contingency plan identified during testing, as needed.
Discussion	Methods for testing HVA contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations should conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.
Related Controls	AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2
References	FIPS 199, NIST SP 800-34, NIST SP 800-84
CSF Function Mapping	Protect

CP-7 ALTERNATE PROCESSING SITE

Control Selection Rationale	Alternate, physical processing sites are critical to continuity of the HVA services in the event of disruption or reduced operational capabilities at a primary processing site. A pre-planned alternate processing site reduces the HVA downtime due to primary processing site functional degradation or failure.
Control Direction:	The organization should:
Item a	establish a physical alternate processing site, including necessary agreements to permit the transfer and resumption of the HVA operations for essential missions and business functions, within the time period as set forth within the organization's contingency plan;
Item b	ensure the equipment and supplies required to transfer and resume operations are available at the alternate site or put contracts in place to support delivery to the site within the organization-defined time-period for transfer and resumption; and
Item c	implement security controls at the alternate processing site equivalent to those at the primary site.
Discussion	Alternate processing sites are sites that are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives such as failover to a cloud-based service provider or other internally- or externally-provided processing service. Geographically distributed architectures that support contingency requirements may also be considered as alternate processing sites. Controls that are covered by alternate processing site agreements include the

	environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions and business functions despite disruption, compromise, or failure in organizational systems. This control may not be necessary for HVAs that are rated as 'Low' impact for availability.
Related Controls	CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13
References	NIST SP 800-34
CSF Function Mapping	Protect, Recover

CP-7 (3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

Control Selection Rationale	Priority-of-service agreements provide organizations with priority treatment consistent with the organization's availability requirements (as prescribed within the organization's contingency plan) for a logical and/or physical alternate processing site.
Control Direction:	The organization should develop alternate processing site agreements that contain priority-of-service provisions in accordance with organizational HVA availability requirements (including HVA recovery time objectives). The organization should establish recovery time objectives as part of contingency planning.
Discussion	Priority-of-service agreements refer to negotiated agreements with service providers that provide organizations with priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site.
Related Controls	N/A
References	NIST SP 800-34
CSF Function Mapping	Protect, Recover

CP-9 (1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

Control Selection Rationale	Ensuring that complete functions of the HVA can be restored and rebuilt is critical in the execution of HVA contingency planning processes to ensure critical systems resiliency.
Control Direction:	The organization should, as part of the contingency planning processes, restore complete select HVA functions to ensure that

	backups are effective, personnel know how to perform function restores, and the function operates correctly once restored.
Discussion	Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.
Related Controls	CP-4
References	OMB Circular A-130, NIST SP 800-34
CSF Function Mapping	Recover

CP-10 (4) SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME-PERIOD	
Control Selection Rationale	The loss of operational functionality of the system to provide mission services must be identified and contingency plans for timely restoration developed.
Control Direction:	The organization should determine, develop, and implement the capability to restore the HVA within a defined restoration time in accordance with organizational HVA availability impact risk assessment.
Discussion	Restoration of HVA components includes reimaging which restores the components to known, operational states.
Related Controls	CM-2, CM-6
References	OMB Circular A-130, NIST SP 800-34
CSF Function Mapping	Recover

Identification and Authentication (IA)

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	
Control Selection Rationale	Identification and authentication capabilities increase user accountability of HVA users and reduces the risk of unauthorized users gaining access to the HVA.
Control Direction:	The organization should implement identification and authentication capabilities that enables the HVA to uniquely identifies all users, systems, and services acting on behalf of organizational users.

Discussion	Each user is uniquely identified with multifactor authentication. Password only authenticators for users or privileged accounts and group/shared accounts are not allowed for access to the HVA. System and Service accounts should not utilize well known account identifications (IDs) (e.g., system administrator (SA), root, administrator, etc.). System and service accounts are only used as intended and authorized. HVA users are not permitted to logon to any system using the system or service accounts. User accounts are not to be used as a system or service account.
Related Controls	AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8
References	OMB Circular A-130, OMB M-19-03, OMB M-11-11, FIPS 201, NIST SP 800-63
CSF Function Mapping	Protect

IA-2 (1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS	
Control Selection Rationale	Privileged accounts are high value targets of malicious actors and protecting them using stronger authentication solutions decreases the threat of compromise through unauthorized access.
Control Direction:	The organization should authenticate all privileged accounts each HVA using multifactor authentication mechanisms to protect against password weaknesses. The HVA and/or HVA components supports and implements authentication of privileged accounts through multifactor authentication.
Discussion	Multifactor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator or cryptographic private key stored in hardware or software), or something you are (e.g., a biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multifactor options appropriate for the level of risk. Organizations can add additional

	security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.
Related Controls	AC-5, AC-6
References	OMB Circular A-130, OMB M-19-03, OMB M-11-11, FIPS 201, NIST SP 800-63
CSF Function Mapping	Protect

IA-2 (2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) \| MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

Control Selection Rationale	Threats and vulnerabilities to password-based authentication drives the requirement for multifactor authentication mechanisms to reduce the possibility of unauthorized/compromised access to the systems.
Control Direction:	The organization should authenticate non-privileged accounts on each HVA using multifactor authentication mechanisms to protect against password weaknesses.
Discussion	All systems and devices support and implement authentication of non-privileged accounts through multifactor authentication. Multifactor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a PIN), something you have (e.g., a physical authenticator or cryptographic private key stored in hardware or software), or something you are (e.g., a biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the DoD CAC. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access, privileged accounts are authenticated using multifactor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.
Related Controls	AC-5
References	OMB Circular A-130, OMB M-19-03, OMB M-11-11, FIPS 201, NIST SP 800-63
CSF Function Mapping	Protect

IA-2 (12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) \| ACCEPTANCE OF PIV CREDENTIALS

Control Selection Rationale	Homeland Security Presidential Directive (HSPD) 12 requires federal agencies to implement PIV credentials for identification and authentication.
Control Direction:	User identification and authentication for the HVA should be facilitated using PIV, in accordance with FIPS Publication 201-1 and OMB M-11-11. Additional authentication factors should be employed in a risk-based manner.
Discussion	Acceptance of PIV-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using (NIST SP 800-79-2). Acceptance of PIV-compliant credentials includes derived PIV credentials, the use of which is addressed in (NIST SP 800-166). The DOD CAC is an example of a PIV credential.
Related Controls	N/A
References	OMB Circular A-130, OMB M-19-03, OMB M-11-11, FIPS 201, NIST SP 800-63
CSF Function Mapping	Protect

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control Selection Rationale	Device authentication protects against unauthorized devices from accessing HVA information and services within the HVA environment.
Control Direction:	The organization should validate the security posture, uniquely identify, and authenticate devices before establishing a network connection to the HVA.
Discussion	Devices that require unique device-to-device identification and authentication are defined by type, by device, or by a combination of type and device. Organization-defined device types can include devices that are not owned by the organization. Systems use shared known information (e.g., MAC and Transmission Control Protocol (TCP)/IP addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-TLS authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations should determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on large scale,

	organizations can restrict the application of the control to a limited number (and type) of devices based on need
Related Controls	AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4
References	OMB Circular A-130
CSF Function Mapping	Protect

IA-5 AUTHENTICATOR MANAGEMENT

Control Selection Rationale	Ensuring an adequate level of security through management of account authenticators is necessary to protect HVA from unauthorized access due to a compromised authenticator.
Control Direction:	The organization should:
Item f	change and/or refresh HVA-related authenticators at least annually or upon departure of key personnel with knowledge of password for service and system account passwords/pins and at least annually for cryptographic devices.
Discussion	Authenticators include passwords, cryptographic devices, one-time password devices, and key cards. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements about authenticator content contain specific characteristics or criteria (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum-length passwords, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related Controls	AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4
References	OMB Circular A-130, OMB M-19-03, OMB M-11-11, FIPS 201, NIST SP 800-63
CSF Function Mapping	Protect

IA-5 (1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION	
Control Selection Rationale	Weak passwords for HVA access can lead to unauthorized access through a compromised or cracked password.
Control Direction:	The organization should ensure that user and privileged HVA accounts comply with multi-factor authentication requirements. HVA service and system accounts that leverage password based authentication should meet the following requirements: Passphrases consist solely of letters twenty or more characters in length, default authentication credentials are not used, passwords must be changed at least annually, or upon personnel turnover; passwords should be stored in a secured location and only used when necessary, passwords should be unique for each identifier and on each system within the HVA boundary, and password reuse is not permitted.
Discussion	Password-based authentication applies to passwords regardless of whether they are used in single-factor or multifactor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefit while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically-protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly-used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context specific words, for example, the name of the service, username, and derivatives thereof.
Related Controls	IA-6
References	OMB Circular A-130, OMB M-19-03, OMB M-11-11, FIPS 201, NIST SP 800-63, NIST SP 800-132
CSF Function Mapping	Protect

Incident Response (IR)

IR-4 (2) INCIDENT HANDLING | DYNAMIC RECONFIGURATION	
Control Selection Rationale	Organizations can rapidly respond to incidents affecting the confidentiality, integrity, and availability of the HVA and HVA components through dynamic reconfiguration. Dynamic reconfiguration reduces the window of time for a threat actor to maliciously exploit an incident.
Control Direction:	The organization should implement dynamic reconfiguration capabilities to HVA(s) or to the HVA components critical to the function(s) of the system. Dynamic reconfiguration capabilities should be included as part of the organization's overall HVA incident response capabilities.
Discussion	The agency may dynamically change router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may also perform dynamic reconfiguration of HVAs to stop attacks, misdirect attackers, or to isolate HVA components, thus limiting the extent of the damage from breaches or compromises. The organization may also re-assign cyber defense responsibilities to personnel or operating centers to manage risks. Organizations should include time frames for achieving the reconfiguration of HVAs in the definition of the reconfiguration capability.
Related Controls	AC-2, AC-4, CM-2
References	NIST SP 800-61 Rev 2, NIST SP 800-86, NIST SP 800-101, NIST SP 800-150, NIST SP 800-160 v2, NIST SP 800-184
CSF Function Mapping	Detect, Respond, Recover

IR-4 (8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS	
Control Selection Rationale	A complete incident response program that addresses all aspects incident response management to include collaboration with external organizations is crucial in ensuring prompt and effective incident response.
Control Direction:	The organization should incorporate external interconnected entities to ensure collaboration and reporting of appropriate information in the HVA incident response plans. ISA/MOU/MOAs should include incident response requirements and reporting timeframes for all entities that interoperate with the HVA in accordance with US-CERT Federal Incident Notification Guidelines.
Discussion	The coordination of incident information with external organizations, including mission or business partners, military or coalition partners, customers, and developers, can provide significant benefits. Cross-

	organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization’s operations, assets, and individuals.
Related Controls	AU-16, PM-16
References	OMB Circular A-130, NIST SP 800-61 Rev 2
CSF Function Mapping	Detect, Respond, Recover

IR-4 (10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION

Control Selection Rationale	The organization can increase incident response effectiveness by coordinating incident response with other organizations in its supply chain.
Control Direction:	The organization should coordinate incident handling activities involving HVA and HVA component-related supply chain events with other organizations involved in the supply chain.
Discussion	Other organizations involved in supply chain activities include product developers, HVA system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include compromises or breaches that involve HVA components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations should consider including processes for protecting and sharing incident information in information exchange agreements. Coordination activities include sharing security and/or privacy incident information to the provider of the HVA or HVA service or other organizations involved in the supply chain for the HVA or HVA components related to the incident.
Related Controls	CA-3, IR-6 (3), MA-2, SA-9, SR-8,
References	NIST SP 800-61 Rev 2, NIST SP 800-86 NIST SP 800-101, NIST SP 800-150 NIST SP 800-160 v2, NIST SP 800-184, NISTIR 7559
CSF Function Mapping	Detect, Respond, Recover

IR-5 INCIDENT MONITORING

Control Selection Rationale	Recording actions and events related to incident response activities streamlines organizational response to incidents and ensures accuracy of records and reporting.
Control Direction:	The organization should monitor, track, and report incidents accurately

	in accordance with US-CERT Federal Incident Notification Guidelines. Organizations should monitor all interconnected traffic into and out of the HVA to detect threats, and abnormal or malicious communications. They also monitor and analyze current threat information sources, emerging vulnerabilities and exploits, latest social engineering tactics, intrusion detection signatures and incorporates pertinent information into their monitoring solutions.
Discussion	Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics. It also includes evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.
Related Controls	AU-6, AU-7, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7
References	OMB Circular A-130, NIST SP 800-61 Rev 2, US-CERT Federal Incident Notification Guidelines
CSF Function Mapping	Detect, Respond

Media Protection (MP)

MP-6 MEDIA SANITIZATION	
Control Selection Rationale	Organizations can reduce the risk of HVA data loss stemming from unauthorized HVA media access by properly sanitizing the media.
Control Direction:	The organization should:
Item a	sanitize media that contains HVA data prior to disposal, release out of organizational control, or release for reuse in accordance with the organization's sanitization procedures; and
Item b	employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the HVA information contained within the media.
Discussion	Media sanitization applies to all digital and non-digital HVA system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media such as paper and microfilm. The sanitization process removes information from HVA system media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, deidentification of personally identifiable information, and destruction, prevent the disclosure of information to

	unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NARA policies controls the sanitization.
Related Controls	AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11
References	OMB Circular A-130, FIPS 199, NIST SP 800-60 v1, NIST SP 800-60 v2, NIST SP 800-88, NIST SP 800-124, NISTIR 8023, NSA Media Destruction Guidance
CSF Function Mapping	Protect

MP-6 (8) MEDIA SANITIZATION | REMOTE PURGING OR WIPING OF INFORMATION	
Control Selection Rationale	Organizations can employ remote HVA purge/wipe capabilities to protect against HVA data loss in the event that the HVA or its component have been obtained by unauthorized individuals.
Control Direction:	The organization should employ the capability to remotely purge or wipe the HVA system and component in the event that the HVA or its component has been obtained by unauthorized individuals.
Discussion	Remote purging or wiping of information protects information on the HVA system and component if either are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the HVA system or component. The purge or wipe function can be implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted HVA data.
Related Controls	N/A
References	OMB Circular A-130, FIPS 199, NIST SP 800-60 v1, NIST SP 800-60 v2, NIST SP 800-88, NIST SP 800-124, NISTIR 8023, NSA Media Destruction Guidance
CSF Function Mapping	Protect

Physical and Environmental Protection (PE)

PE-3 PHYSICAL ACCESS CONTROL	
Control Selection Rationale	Physical access to HVA systems and environment is risk-based to protect against to consequences of unauthorized physical access to the systems.
Control Direction:	The organization should authorize physical access to HVA systems and environment using dual authorizations. Physical access to environments housing HVA components requires two authorized individuals within the organization to approve a requestor's physical access to HVA. Physical Access requests are reauthorized at least annually.
Discussion	Physical access control applies to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Organizations should determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems requiring supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.
Related Controls	AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3
References	OMB Circular A-130, FIPS 201
CSF Function Mapping	Protect, Detect

PE-3 (1) PHYSICAL ACCESS CONTROL | SYSTEM ACCESS	
Control Selection Rationale	Protecting and limiting access to physical spaces containing HVA systems ensures the confidentiality, integrity, and availability of the system and information.
Control Direction:	The organization should enforce physical access authorization along with physical access controls for the facilities where the HVA components and systems reside. For physical locations where numerous other non-HVA systems are co-located, organizations consider restricting access to the cabinet/rack containing the HVA devices.
Discussion	Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Related Controls	N/A
References	OMB Circular A-130, FIPS 201
CSF Function Mapping	Protect, Detect

Planning (PL)

PL-2 SYSTEM SECURITY AND PRIVACY PLANS	
Control Selection Rationale	HVA Security and Privacy Plans should provide specific details regarding the implementation of the system and the rationale for the selection of security controls to protect the HVA from threats.
Control Direction:	The organization should develop HVA Security and Privacy plans that contain sufficient information to protect the confidentiality, integrity, and availability of the HVA.
Discussion	Descriptions of tailored controls should include a detailed justification as to why the control was included or not and how it has been implemented. Control descriptions inherited from another system should also provide sufficient detail regarding how the control implementation meets control requirements for the HVA. HVA Security and Privacy plans should include at least the following: Security Categorization and supporting rationale, authorization boundary of the HVA, description of the HVA from a mission and business perspective, detailed description of the HVA operational environment, detailed interconnection information, description of the HVA protection needs, relevant overlays used (e.g., HVA, Privacy, etc.), control tailoring details and supporting rationale, and detailed description of the implementation of each security control. In accordance with CA-6(1) as defined in this overlay, the HVA Security and Privacy Plan are to be authorized and signed following the Joint Authorization method.
Related Controls	AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4
References	OMB Circular A-130, NIST SP 800-18
CSF Function Mapping	Protect, Detect

PL-8 SECURITY AND PRIVACY ARCHITECTURES	
Control Selection Rationale	The architecture of the HVA environment should protect the information and supported missions from loss of confidentiality, integrity or

	availability. The architecture should also be designed and implemented to protect the systems and information that comprise the HVA from external collocated systems and internal HVA components that are a higher risk posture (e.g., Internet facing systems).
Control Direction:	The organization should implement architectures designed to protect the security and privacy of the HVA and HVA data from potential compromise.
Discussion	In accordance with OMB M-19-03, organizations should ensure the following are being implemented: strict access control, multifactor authentication vulnerability scanning increased monitoring and analysis of events, network segmentation, boundary protections, and incident response testing. The HVA security architecture should be designed and implemented in a layered approach based on risk assessment of threats to components and data, information flow, user access, insider threats, operational behaviors, and mission critical services. Detailed data flows of information within the HVA should be developed and prioritized, and rules and policies should be created where segmentation and layers of isolation are identified. Devices that do not require direct access by HVA users should be located behind boundary protection devices with strict access control, filtering, and monitoring. Access lists should be set to default deny and permit by exception both inbound and outbound. Egress rules should block all access except required services and block all unnecessary traffic to the Internet. Security and administrative services and functions should be isolated onto their own networks with strict access control. The organization should implement access control lists to limit traffic between security, admin, and production networks. Traffic entering and leaving the HVA accreditation boundary should be encrypted in accordance with the risk analysis of the information being transmitted. Device services and applications should only be bound to the appropriate interface/network required for it to function.
Related Controls	CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17
References	OMB Circular A-130, NIST SP 800-160
CSF Function Mapping	Identify, Protect

PL-8 (1) SECURITY AND PRIVACY ARCHITECTURES | DEFENSE-IN-DEPTH

Control Selection Rationale	Protecting HVA data behind multiple layers of security boundaries ensures that adversaries must circumvent multiple security mechanisms before compromising HVA data and services.
Control Direction:	The organization should implement multiple layers of security to increase the security of HVAs.
Discussion	Leveraging risk assessments, organizations protect information and mission critical services through a defense-in-depth approach for systems and information using multiple layers of security protections. Examples of the multiple layers are shown in Figure 2: Web Zone, Application Zone, and Data Zone. Flow control and access control lists are implemented between layers using security safeguards, boundary protection devices, proxy servers, application gateways, intrusion prevention/detection etc. Figure 2 depicts firewalls controlling access between the tiered layers. These firewalls are also used to monitor traffic for malicious content, unauthorized access, inside threats, and exfiltration.
Related Controls	SC-2, SC-3, SC-29, SC-36
References	OMB Circular A-130, NIST SP 800-160
CSF Function Mapping	Identify, Protect

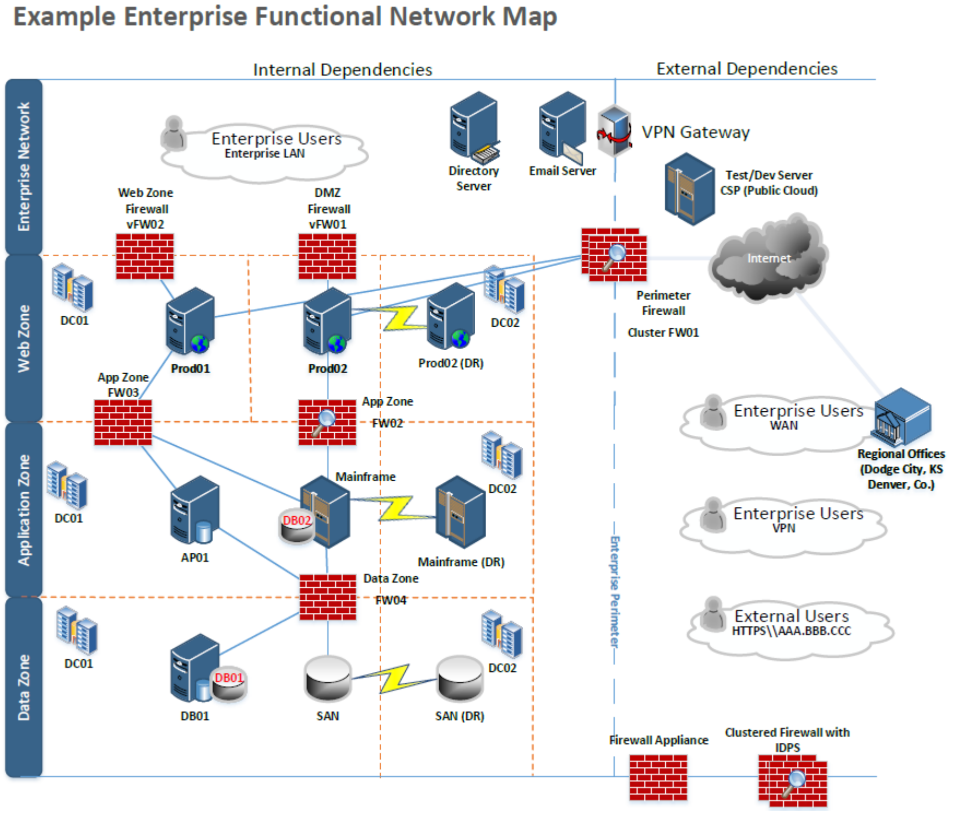


Figure 2. Sample Architecture

PL-10 BASELINE SELECTION	
Control Selection Rationale	Security categorization of HVAs are performed in accordance with FIPS 199. Additional controls for HVA systems should be applied in a risk-based manner in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and the Privacy Act to ensure sufficient security measures are implemented to protect HVAs.
Control Direction:	The organization should implement at least the Moderate baseline from NIST SP 800-53 Rev 5. All HVA overlay controls should be applied as specified and not tailored.
Discussion	Organizations should leverage FIPS 199 system categorization to select and tailor the initial baseline controls for HVA from NIST SP 800-53 Rev 5 (Moderate or High baselines only). All HVA systems should also implement the controls in the HVA overlay. Based on a risk assessment and the types of information stored, transmitted. And processed by the HVA, additional overlays may be necessary and other controls tailored in or out in accordance with the NIST Risk Management Framework.
Related Controls	PL-2, PL-11, RA-2, RA-3, SA-8
References	OMB Circular A-130, FIPS 199
CSF Function Mapping	Identify, Protect

Personally Identifiable Information Processing and Transparency (PT)

PT-3 (1) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | DATA TAGGING	
Control Selection Rationale	Data tags enable HVA operators to track PII and the processing purpose(s) of the PII as it traverses the HVA. HVA operators can identify whether a change in processing would be compatible with the identified and documented purposes (i.e. processing through an alternate HVA system).
Control Direction:	The organization should attach data tags to data that contains the relevant elements of PII along with the purpose(s) of tracking the PII processed by the HVA(s).
Discussion	Data tags support tracking of processing purposes by conveying the purposes along with the relevant elements of personally identifiable information throughout the system. Data tags may also support the use of automated tools. The authority to process PII is documented in privacy policies and notices, system of record notices, privacy impact assessments, Privacy Act statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.
Related Controls	CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19
References	Privacy Act, OMB Circular A-130, Appendix II

CSF Function Mapping	Identify

PT-3 (2) PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | AUTOMATION	
Control Selection Rationale	Automated data tag tracking capabilities reduces the labor requirements and errors associated with manual data tag tracking.
Control Direction:	The organization should track the processing purposes of personally identifiable information through the HVA using an automated tool.
Discussion	Automated mechanisms augment tracking of the processing purposes.
Related Controls	CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19
References	Privacy Act, OMB Circular A-130, Appendix II
CSF Function Mapping	Identify

Risk Assessment (RA)

RA-2 SECURITY CATEGORIZATION	
Control Selection Rationale	To provide the necessary level of assurance to stakeholders, organizations should categorize the HVA at the appropriate level to ensure protection of the HVA information, systems, components, and mission critical services congruent with the information being stored, transmitted, and processed on the system.
Control Direction:	The organization should apply the "high water mark" concept to their HVA systems by properly categorizing HVAs and at least no lower than a Moderate based on the definition of the impacts defined in FIPS 199.
Discussion	Clearly defined HVA system boundaries are a prerequisite for security categorization decisions. Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are comprised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in the systems security engineering processes carried out throughout the system development life cycle.
Related Controls	CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12
References	OMB Circular A-130, FIPS 199, NIST SP 800-30, NIST SP 800-37, NIST SP 800-60.
CSF Function Mapping	Identify

RA-3 (1) RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT		
Control Selection Rationale		Organizations can identify and reduce risks posed via the supply chain by conducting supply chain risk assessments.
Control Direction:		The organization should:
	Item a	assess supply chain risks associated with the HVA, HVA components, and HVA system services; and
	Item b	review and/or update the supply chain risk assessment at least annually, when there are significant changes to the relevant supply chain, or when changes to the HVA, environments of operation, or other conditions may necessitate a change in the supply chain.
Discussion		Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.
Related Controls		RA-2, RA-9, PM-17, SR-2
References		RA-5(10), NIST SP 800-40, NIST SP 800-53A, NIST SP 800-70, NIST SP 800-115, NIST SP 800-126, NISTIR 7788, NISTIR 8023
CSF Function Mapping		Identify, Protect, Detect, Respond

RA-5 VULNERABILITY MONITORING AND SCANNING	
Control Selection Rationale	Timely identification of vulnerabilities in the HVA is critical to ensuring HVA systems and components are protected from compromise due to those vulnerabilities.
Control Direction:	The organization should consider performing credentialed agent-based or credentialed workstation-based vulnerability scans to comply with a 72-hour scanning recommendation discussed below.
Discussion	Per CDM requirements, organizations should implement vulnerability scanning capabilities to discovery and identify known flaws on the components at least every 72 hours. Security categorization of information and systems guide the frequency and comprehensiveness of vulnerability

	monitoring (including scans). Organizations should determine the required vulnerability monitoring for system components, ensuring the potential sources of vulnerabilities such as infrastructure components (e.g., switches, routers, sensors), networked printers, scanners, and copiers are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced, and as new scanning methods are developed, helps to ensure new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure potential vulnerabilities in the system are identified and addressed as quickly as possible.
Related Controls	CA-2, CA-7, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11
References	OMB Circular A-130, CISA CDM program
CSF Function Mapping	Identify, Protect, Detect, Respond

RA-5 (6) VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSIS

Control Selection Rationale	Organizations can determine HVA vulnerability trends and relationships by analyzing scan results from automated vulnerability scanning capabilities or mechanisms.
Control Direction:	The organization should compare the results of multiple HVA vulnerability scans using its implemented automated HVA vulnerability scanning capability.
Discussion	The organization can choose to compare scans from a single HVA or scans that were completed across multiple HVAs if broader trend analysis is desired. This process can help the organization correlate scanning information, as described in RA-5(10).
Related Controls	N/A
References	RA-5(10), NIST SP 800-40, NIST SP 800-53A, NIST SP 800-70, NIST SP 800-115, NIST SP 800-126, NISTIR 7788, NISTIR 8023
CSF Function Mapping	Identify, Protect, Detect, Respond

RA-5 (10) VULNERABILITY MONITORING AND SCANNING | CORRELATE SCANNING INFORMATION

Control Selection Rationale	Organizations can more effectively identify HVA attack vectors and vulnerabilities by correlating HVA vulnerability scan results.
Control Direction:	The organization should correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and

	multi-hop attack vectors that could be used to attack the HVA.
Discussion	An attack vector is a path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors. The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and create opportunities for adversary exploitation. Organizations can correlate both previous and current vulnerability scan results, as well as results from different HVAs that may be configured (e.g., applications, active network connects) in a similar manner.
Related Controls	N/A
References	NIST SP 800-40, NIST SP 800-53A, NIST SP 800-70, NIST SP 800-115, NIST SP 800-126, NISTIR 7788, NISTIR 8023, RA-5 (6)
CSF Function Mapping	Identify, Protect, Detect, Respond

System and Services Acquisition (SA)

SA-4 ACQUISITION PROCESS	
Control Selection Rationale	Contracts for HVA system support, services, and solutions should comply with security requirements of the Federal Government and relevant organizational policies and procedures to ensure the contractors are protecting the information and systems at the appropriate levels.
Control Direction:	The organization should ensure contract agreements for support or services of HVA systems and environment include requirements for the application of the HVA control overlay. Contractor agreements should incorporate Federal Incident Reporting Guidelines, as identified by US-CERT, into Service Level Agreements.
Discussion	All contract agreements for support or services of HVA systems or services include the relevant language from the Federal Acquisition Regulation (FAR) Section 7.103 containing information security requirements from FISMA. Contractors should comply with all security requirements as defined in the contractual agreements. The organization should oversee and monitors the contractor's compliance with the contract.

Related Controls	CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5
References	OMB Circular A-130, NIST SP 800-37, NIST SP 800-137
CSF Function Mapping	Protect, Detect

SA-9 EXTERNAL SYSTEM SERVICES

Control Selection Rationale		Ensuring external services providers and contractors comply with federal, department, and agency security requirements protects the information and systems from unauthorized compromise or loss of availability.
Control Direction:		The organization should:
	Item a	require providers of external services comply with organizational security and privacy requirements and comply with the specifications defined in the HVA control overlay.
Discussion		External system services are services that are provided by an external provider and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. Organizations should establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. Organizations should document the basis for the trust relationships so the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements.
Related Controls		AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5
References		OMB Circular A-130
CSF Function Mapping		Identify, Protect, Detect

SA-11 DEVELOPER TESTING AND EVALUATION

Control Selection Rationale	Documenting and testing security and privacy controls during the development of the application or system ensures security is built into the solution and that the controls are operating as intended.
Control Direction:	The organization should require developers of system, components, or solutions to create and document security testing plans and test all required security controls during development, including the HVA overlay controls.

Discussion	Developmental testing and evaluation can confirm the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes, including upgrading or replacing applications, operating systems, and firmware, may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws.
Related Controls	CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

SA-11 (1) DEVELOPER TESTING AND EVALUATION | STATIC CODE ANALYSIS

Control Selection Rationale	Performing analysis on static code to detect weaknesses or flaws in the code protects against unauthorized access, loss of integrity, or loss of availability to the HVA.
Control Direction:	The organization should ensure static code analysis is performed on applications to identify code weaknesses and outdated or vulnerable libraries as part of the development lifecycle. Contractual language for contractor development requires the contractor to perform this task as part of the deliverables. Organizations should also require static code analysis for all modifications, updates, or additions to applications or systems prior to implementation.
Discussion	Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code and checking for incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Static code analysis can be used to identify vulnerabilities and to enforce secure coding practices and is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static code analysis can provide clear remediation guidance along with defects to enable developers to fix such defects.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

SA-11 (2) DEVELOPER TESTING AND EVALUATION | THREAT MODELING AND VULNERABILITY ANALYSIS

Control Selection Rationale	Testing for vulnerabilities and performing threat modeling during the development lifecycle of a system or application ensures the solution being developed is incorporating the required security capabilities and operating as intended.
Control Direction:	The organization should require threat modeling and vulnerability analyses prior to deployment to ensure that design and implementation changes have been accounted for, and vulnerabilities created as a result of those changes have been reviewed and mitigated. Organizations should incorporate threat modeling and vulnerability analysis requirements in contractual language for new and updates/upgrades/changes to existing applications. Organizations should also monitor and track contractor compliance with contractual requirements.
Discussion	Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design stages of the HVA system development life cycle. Therefore, updates to threat modeling and vulnerability analyses of those systems, system components, and system services during development and prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this stage of the system development life cycle ensure design and implementation changes have been accounted for and vulnerabilities created because of those changes have been reviewed and mitigated.
Related Controls	PM-15, RA-3, RA-5
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

SA-11 (4) DEVELOPER TESTING AND EVALUATION | MANUAL CODE REVIEWS

Control Selection Rationale	Manual code review of components and applications can identify issues, weaknesses, or defects not detectable by automated means (authentication issues, cryptographic challenges, etc.). These manual code reviews protect against potential loss in confidentiality, integrity, and availability of HVA systems.
Control Direction:	The organization should require developers of applications or components to perform manual code review as part of the system development lifecycle through organizational policies, contractual language requirements, and deliverables. Organizations should monitor and track contractor compliance with organizational policies and contractual requirements for manual code review.
Discussion	Manual code reviews are usually reserved for the critical software and firmware components of systems. They are effective in identifying weaknesses that require knowledge of the application's requirements or context which in most cases, are unavailable to automated analytic

SA-11 (4) DEVELOPER TESTING AND EVALUATION | MANUAL CODE REVIEWS

	tools and techniques, for example, static and dynamic analysis. The benefits of manual code review include the ability to verify access control matrices against application controls and review detailed aspects of cryptographic implementations and controls.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

SA-11 (5) DEVELOPER TESTING AND EVALUATION | PENETRATION TESTING

Control Selection Rationale	The organization can protect against loss of confidentiality, integrity, and availability by testing new or modified applications or components prior to implementation on the HVA.
Control Direction:	The organization should require developers of applications or components to perform penetration test, prior to implementation, against new and updates, upgrades, or changes to applications or components as part of the contractual requirements. Organizations should define policy and processes around expediting critical patches as necessary based on risk assessments. The purpose of penetration testing is to identify potential vulnerabilities in solution resulting from development errors, configuration faults, or other operational weaknesses or deficiencies. Penetration testing is often performed in conjunction with automated and manual code reviews to provide greater levels of analysis. Organizations should monitor and track contractor compliance with contractual requirements.
Discussion	Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent implemented security and privacy features of information technology products and systems. The objective of penetration testing is to discover vulnerabilities in systems, system components and services resulting from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.
Related Controls	CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

SA-11 (8) DEVELOPER TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS

Control Selection Rationale	Reviewing and analyzing code dynamically to detect flaws, vulnerability, or code defects protects against possible loss of confidentiality, integrity, and availability.
Control Direction:	The organization should require developers of applications or components to perform dynamic code analysis during the system development lifecycle and prior to implementation as part of organizational policies and contractual agreements. Dynamic code analysis typically leverages automated tools to test security functionality to verify the effectiveness of the security. An example includes fuzz testing which induces intentional program failures by using malformed or random data injection into software programs. Organizations should monitor and track contractor compliance with organizational policies and contractual requirements.
Discussion	Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to ensure that security functionality performs in the way it was designed. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis and/or concordance analysis.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect

System and Communications Protection (SC)

SC-3 SECURITY FUNCTION ISOLATION	
Control Selection Rationale	Comingling security operations network traffic with production network traffic could lead to the loss of integrity of the security traffic due to a compromise of the system.
Control Direction:	The organization should isolate security communications from production functions on networks to provide additional protection to security communications. Organizations should consider and address risks to security communications by establishing multiple network connections to isolated network and accounting for the potential of lateral movements through backend networks connections. Following the principle of least functionality system must be configured to bind services to only the network interfaces necessary for them to function. For example, an external web service should only be bound to the external facing network interface and not to all interfaces on the system as there is no need for the web service to be accessible on

	the security communications interface.
Discussion	Security functions are isolated from non-security functions by means of an isolation boundary implemented via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Systems implement code separation in many ways and can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the recommendation is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions within the isolation boundary as an exception. The isolation of security functions from non-security functions can be achieved by applying the systems security engineering design principles in SA-8 including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).
Related Controls	AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16
References	OMB Circular A-130
CSF Function Mapping	Identify

SC-3 (2) SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS	
Control Selection Rationale	Controlling and protecting access to and flow control for security functions further protects the integrity of the security information of the system.
Control Direction:	The organization should implement access and flow control to and from the security functions network and other network(s) supporting the HVA environment. Organizations should ensure that multi-homed hosts do not allow lateral movement due to backend support networks through access and flow control. Examples of security functions that should be isolated using access and flow control are auditing, intrusion detection, and anti-virus functions.
Discussion	Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include auditing, intrusion detection, and malicious code protection functions.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Identify

SC-5 DENIAL OF SERVICE PROTECTION	
Control Selection Rationale	The organization can implement denial of service (DoS) protection to ensure availability of the HVA and protect external facing HVAs against denial of service attacks.
Control Direction:	The organization should determine if the denial of service protection is to be applied at the perimeter of the HVA authorization boundary, at the perimeter of the organization's enterprise network, or both locations based on risk assessment of the potential threats to the HVA's availability.
Discussion	DoS events may occur due to a variety of internal and external causes such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a variety of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial of service events. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial of service events.
Related Controls	CP-2, IR-4, SC-6, SC-7, SC-40
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect, Detect

SC-5 (1) DENIAL OF SERVICE PROTECTION | RESTRICT ABILITY TO ATTACK OTHER SYSTEMS	
Control Selection Rationale	DoS attacks can be launched from inside the organization either intentionally or accidentally. DoS protections applied to the authorization boundary perimeter and at key points inside the authorization boundary protects against loss of availability due to intentional or accidental attacks from organizational users located outside the HVA boundary.
Discussion	Restricting the ability of individuals to launch denial of service attacks requires the mechanisms commonly used for such attacks be unavailable. Organizations should restrict the ability of individuals to connect and transmit arbitrary information on the transport medium and should limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific systems or on boundary devices prohibiting egress to potential target systems.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect, Detect

SC-5 (2) DENIAL OF SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY	
Control Selection Rationale	Not limiting or managing capacity, bandwidth, and redundancy at the authorization boundary and inside the boundary can lead to a loss of availability due to lack of network resources.
Control Direction:	The organization should limit and control capacity into and out of the authorization boundary and at key points inside the boundary to ensure sufficient capacity exists to prevent network flooding DoS. Organizations should perform a risk assessment to determine the appropriate locations inside the authorization boundary based on data flow and user access.
Discussion	Managing capacity ensures sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect, Detect

SC-5 (3) DENIAL OF SERVICE PROTECTION | DETECTION AND MONITORING

Control Selection Rationale	Monitoring boundary protection devices for indicators of DoS attacks allows the organization to respond to denial of service attacks in a timely manner, thereby reducing or avoiding a loss of availability.
Control Direction:	The organization should:
Item a	employ inspection tools to detect DoS anomalies both at the perimeter of the authorization boundary as well as inside the authorization boundary on access control points that form isolation zones; and
Item b	monitor HVA system resources to determine if enough protections exist to prevent effective DoS attacks. The organization should determine the level of inspection required for each isolation zone based on risk assessment to the HVA.
Discussion	Organizations should consider utilization and capacity of system resources when managing risk from denial of service due to malicious attacks. DoS attacks can originate from external or internal sources. System resources sensitive to denial of service include physical disk storage, memory, and central processing unit cycles. Controls used to prevent denial of service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.
Related Controls	CA-7, SI-4
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect, Detect

SC-7 BOUNDARY PROTECTION

Control Selection Rationale	Control and isolation of HVA systems and information at the authorization boundary is necessary to protect the information and mission critical services from lateral threats.
Control Direction:	The organization should:
Item a	monitor and control communications at the external interfaces to the system and at key internal interfaces within the system;
Item b	implement subnetworks for publicly accessible system components that are physically/logically separated from internal organizational networks; and
Item c	connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Discussion	The organization should employ boundary protection solutions at the HVA authorization boundary to protect the information and mission critical services from adjacent systems (to include other HVAs) within the organization. HVAs that rely on supporting systems in the enterprise protected at a lower level of trust should be implemented in a manner that reduces the risk these interdependencies may introduce to the HVA. Examples of boundary protection devices include: Firewalls, Application Firewall/Proxy/Gateway (web, email, data transfers, etc.), Intrusion Detection, Service/Intrusion Prevention Services, and Application Load Balancer/Cryptographic services. Organizations should implement default deny, permit by exception for egress and ingress access control at the system boundary. All devices should be explicitly blocked (inbound and outbound) at the authorization boundary and specific access granted for communications based on source IP, destination, IP, port, and protocol. “ANY” or “ALL” rules should not be used in allow access control statements. Systems and components within the HVA environment should not have direct access to the Internet unless specifically required for the application to function. It is recommended to block Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) traffic bi-directionally for all internal systems. Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks physically or logically separated from internal networks are referred to as demilitarized zones. Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions.
Related Controls	AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PM-12, SA-8, SC-5, SC-32, SC-43
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

SC-7 (3) BOUNDARY PROTECTION | ACCESS POINTS

Control Selection Rationale	The organization can reduce the risk of unauthorized network access to an HVA by limiting the number of external network connections to an HVA.

Control Direction:	The organization should limit the number of external network connections to the HVA, maintaining only the minimum number of external network connections required for the HVA to function or provide a service.
Discussion	The Trusted Internet Connection (TIC) initiative is an example of a federal guideline requiring limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system. Limiting external network connections to an HVA also reduces the amount of inbound and outbound communications that must be monitored and analyzed due to fewer active data connections.
Related Controls	N/A
References	OMB A-130, FIPS 199, NIST SP 800-37, NIST SP 800-41, NIST SP 800-77, NIST SP 800-189.
CSF Function Mapping	Identify, Protect, Detect, Respond

SC-7 (5) BOUNDARY PROTECTION | DENY BY DEFAULT - ALLOW BY EXCEPTION

Control Selection Rationale	The organization can reduce the risk of unauthorized access to the HVA via unapproved inbound/outbound HVA connections by allowing only excepted connections to the HVA.
Control Direction:	The organization should deny network communications traffic to the HVA by default and allow network communications traffic by exception at managed interfaces or for authorized organization-defined HVA support systems.
Discussion	Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.
Related Controls	N/A
References	N/A
CSF Function Mapping	Identify, Protect, Detect, Respond

SC-7 (10) BOUNDARY PROTECTION | PREVENT EXFILTRATION

Control Selection Rationale	Safeguarding against intentional and unintentional exfiltration of data from the environment through technical controls and inspection traffic to identify exfiltration protects against potential loss of confidentiality of information.
Control Direction:	The organization should implement technical measures and enhanced inspection of traffic flow into, out of, and within the authorization boundary. Measures such as enforcing protocol validation checking, traffic monitoring, packet inspection, Secure Sockets Layer packet inspection, and beaconing traffic should be implemented on the authorization boundary devices and isolation devices throughout the environment.
Discussion	This control applies to intentional and unintentional exfiltration of information. Controls to prevent exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected or call backs to command and control centers, monitoring for steganography, disassembling and reassembling packet headers, and employing data loss and data leakage prevention tools. The various devices that enforce strict adherence to protocol formats verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.
Related Controls	AC-2, SI-3
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

SC-7 (11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Control Selection Rationale	The organization can limit HVA exposure to threats and reduce the attack surface of the HVA by restricting access through the authorization boundary to only authorized traffic limits.
Control Direction:	The organization should implement incoming communications control for the HVA at the authorization boundary. Access control should be as restrictive and specific as possible. The use of wildcards in ALLOW rules (ANY or ALL) should not be used. Default deny ANY rules with logging should be enabled.
Discussion	General source address validation techniques should be applied to restrict the use of illegal and unallocated source addresses and source addresses that should only be used inside the system boundary. Restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Strong authentication of network addresses

	is not possible without the use of explicit security protocols and thus, addresses can often be spoofed. Also, identity-based incoming traffic restriction methods can be employed to reduce these risks.
Related Controls	AC-3
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

SC-7 (12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

Control Selection Rationale	The organization can protect the HVA from lateral attacks from adjacent systems or direct attacks by implementing host-based protections on the HVA.
Control Direction:	The organization should implement host-based protections (e.g., firewall, Host-Based Intrusion Detection System, Host-Based Intrusion Prevention System) on the HVA system components to protect the HVA from unauthorized access or compromise as part of a defense-in-depth approach. Organizations should monitor these system activities as part of the incident monitoring processes and procedures.
Discussion	Host-based boundary protection mechanisms include host-based firewalls. System components employing host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

SC-7 (14) BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

Control Selection Rationale	HVAs may be co-located (wiring closets, cable distribution closets, etc.) with other devices considered outside the HVA authorization boundary. Protecting against accidental or intentional unauthorized connections to the HVA environment ensures unauthorized connections do not compromise the information, components, and mission critical services.
Control Direction:	The organization should ensure the physical access to network components supporting HVA systems and environments are protected from unauthorized access and unauthorized connection of devices. This protection scheme is based on a risk assessment of the physical environment(s) containing HVA components.
Discussion	HVA systems operating at different security categories or classification levels may share common physical and environmental controls since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment.

	Protection against unauthorized physical connections can be achieved, for example, by using clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items.
Related Controls	PE-4, PE-19
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

SC-7 (17) BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS

Control Selection Rationale	Malicious payloads can be masked inside protocols that are authorized to traverse an HVA boundary. Often these masked packets violate industry defined protocol standards and are easily detected by boundary devices that verify protocol standards.
Control Direction:	The organization should ensure HVA authorization boundary devices and internal boundary devices enforce protocol validation checking bi-directionally for HVA network traffic. (i.e. TCP/IP protocol validation). Nonstandard protocols are identified, addressed, and remediated following POA&M processes.
Discussion	System components that enforce protocol formats include deep packet inspection firewalls and Extensible Markup Language gateways. The components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.
Related Controls	SC-4
References	OMB Circular A-130
CSF Function Mapping	Protect, Detect

SC-7 (21) BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS

Control Selection Rationale	Controlling information flows between components of HVAs restricts and reduces the risk of lateral movement of threats.
Control Direction:	The organization should isolate HVA components to limit lateral movement among those components and provide the capability for increased protection of the entirety of the HVA. Additional security boundaries should be applied inside the HVA authorization boundary to isolate components requiring higher-levels of protections. Isolation

	examples include, enclaving off data repository systems and controlling access so that only necessary services and users can access the data store. Isolation should be established, and access controlled by boundary protection devices. As depicted in Figure 3, isolation can be facilitated using access control points to create multiple zones (web, application, and data zone). Organizations should also implement inspection on access control points to protect HVA data and system components. They should limit access flows outbound and inspect traffic on access control points from the enclaves to protect against exfiltration of data.
Discussion	Organizations can isolate system components performing different missions or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to more effectively control information flows between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyber-attacks and errors.
Related Controls	CA-9, SC-3
References	OMB Circular A-130, NIST SP 800-160
CSF Function Mapping	Protect, Detect

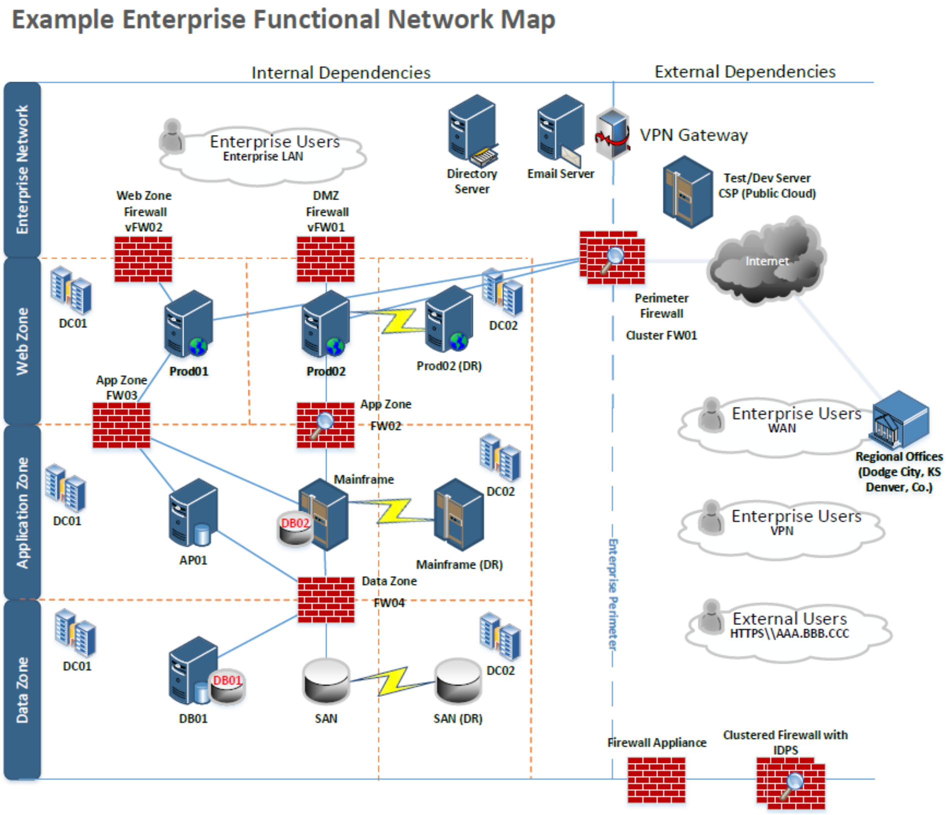


Figure 3. Sample Architecture

SC-7 (22) BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS

Control Selection Rationale	The organization can employ subnetworks (subnets) to protect the HVA when connecting to security domains containing information/systems with security categories or classification levels different from the HVA.
Control Direction:	The organization should implement a subnet containing its HVA and assign this subnet a separate network address to use when connecting to other HVAs or systems in different subnets or security domains.
Discussion	The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains containing information with different security categories or classification levels. The organization may leverage the CDM boundary protection tools and methods to aid in protecting HVA boundaries.
Related Controls	N/A
References	OMB Circular A-130, FIPS 199, NIST SP 800-37, NIST SP 800-41, NIST SP 800-77, NIST SP 800-189, OMB M-19-26
CSF Function Mapping	Protect, Detect

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control Selection Rationale	Due to the sensitivity of HVA data, the confidentiality and integrity of such information must be protected in transit.
Control Direction:	The organization should ensure HVA information traversing a network inside and outside the HVA authorization boundary receives confidentiality and integrity protections. (Minimal encryption in accordance with FIPS 140-2). The HVA system should protect the confidentiality and integrity of transmitted information over trusted and untrusted networks (networks outside the HVA authorization boundary are not trusted).
Discussion	Protecting the confidentiality and integrity of transmitted information applies to internal and external networks, and any system components that can transmit information. Unprotected communication paths are exposed to the possibility of interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services, may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and

	integrity. In such situations, organizations should determine what types of confidentiality or integrity services are available.
Related Controls	AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28
References	OMB Circular A-130, FIPS 140-2, NIST SP 800-77, NIST SP 800-113
CSF Function Mapping	Protect

SC-18 (4) MOBILE CODE | PREVENT AUTOMATIC EXECUTION

Control Selection Rationale	natic execution of code within the HVA protects against malicious code ng the information, system, and mission critical services.
Control Direction:	The organization should protect the HVA by preventing the automatic execution of code on all HVA systems and system components. An example of this is disabling auto run features on system components.
Discussion	Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing automatic execution of mobile code includes disabling auto execute features on system components employing portable storage devices such as Compact Disk, Digital Versatile Disks, and Universal Serial Bus devices.
Related Controls	None
References	OMB Circular A-130
CSF Function Mapping	Detect

SC-28 PROTECTION OF INFORMATION AT REST

Control Selection Rationale	The confidentiality and integrity of HVA data must be protected for data-at-rest (DAR) to prevent unauthorized access or exfiltration of HVA data.
Control Direction:	The organization should ensure the HVA's DAR receive confidentiality and integrity protections such as encryption. This control applies to workstations, servers, database stores, database repositories, information stores, portable media, and share drives.
Discussion	Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information requiring protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authenticator content. When adequate protection of information at rest

	cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure off-line storage in lieu of online storage.
Related Controls	AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16
References	OMB Circular A-130, FIPS 140-2
CSF Function Mapping	Protect

SC-28 (1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

Control Selection Rationale	Cryptographic capabilities protect the confidentiality and integrity of information at rest. This increases the difficulty for threat actors to view or access data residing on the HVA.
Control Direction:	The organize should implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest on the HVA.
Discussion	Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information contained within the HVA. The strength of the cryptographic mechanism should be commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on HVA components or media or encrypt data structures, including files, records, or fields. The organization may leverage CDM Data Protection Management tools and methods to protect HVA information at rest.
Related Controls	AC-19
References	OMB Circular A-130, NIST SP 800-56A, NIST SP 800-56B, NIST SP 800-56C, NIST SP 800-57-1, NIST SP 800-57-2, NIST SP 800-57-3, NIST SP 800-111, NIST SP 800-124, 6 U.S.C. 1523
CSF Function Mapping	Protect

System and Information Integrity (SI)

SI-2 FLAW REMEDIATION

Control Selection	HVA systems and components impacted by announced software vulnerabilities should be identified, a risk assessment performed, and

Rationale	remediated in accordance with organizational policies and procedures. Timely remediation of flaws is required to protect the HVA.
Control Direction:	Per CISA Binding Operational Directive (BOD) 19-02 Vulnerability Remediation Requirements for Internet-Accessible Systems, the organization should develop flaw remediation policies, procedures, and processes for flaw remediation that: prioritizes flaw remediation based on vulnerability exposure and criticality risk, define regular maintenance windows for flaw remediation, tests patches prior to production deployments, include identification and automated inventory of all software, hardware, and firmware and addresses flaws for all items inventoried. Additionally, they should integrate flaw remediation with change management processes and mitigates critical vulnerabilities on Internet facing systems in no more than 15 days.
Discussion	The need to remediate system flaws applies to all types of software and firmware. Organizations should identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Organizations should also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.
Related Controls	CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11
References	OMB Circular A-130, CISA BOD 19-02
CSF Function Mapping	Identify, Protect

SI-3 MALICIOUS CODE PROTECTION

Control Selection Rationale	Malicious code protections for HVA are essential to assure the protection of data and services from compromise, loss of integrity, or loss of availability.
Control Direction:	The organization should ensure automatic antivirus/malware scans of all systems are completed at least biweekly and malicious code detection is blocked, quarantine, and the administrators alerted upon detection.

Discussion	System entry and exit points include firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, trojan horses, and spyware and can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code protection mechanisms include both signature and non-signature-based technologies. In situations where malicious code cannot be detected by detection methods or technologies, organizations should rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure the software does not perform functions other than intended.
Related Controls	AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15
References	OMB Circular A-130
CSF Function Mapping	Detect

SI-4 SYSTEM MONITORING	
Control Selection Rationale	Monitoring the HVA to detect threats or IOC is critical in assuring the protection of the HVA data components from compromise, loss of integrity, and loss of availability.
Control Direction:	The organization should monitor the environment for both internal and external threats leveraging monitoring information from the boundary devices, isolation devices, workstation and server devices, and intrusion/prevention devices. The HVA environment should be monitored for anomalous traffic, exfiltration, and indicators of insider threat. For example, a user copying unordinary large amounts of data as compared to other users should be identified and reviewed.
Discussion	System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at system boundaries while internal monitoring includes the observation of events occurring within the system. Organizations should monitor systems for example, by observing audit activities in cyber-relevant time or by observing other system aspects such as access patterns, characteristics of access, and other actions. System monitoring capability is achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.
Related Controls	AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PM-12, RA-5, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10

SI-4 SYSTEM MONITORING

References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (1) SYSTEM MONITORING | SYSTEM WIDE INTRUSION DETECTION SYSTEM

Control Selection Rationale	System wide intrusion detection/prevention solutions provide a greater view of threats to the environment and allows for better correlation and analysis of incidents.
Control Direction:	The organization should implement HVA environment wide intrusion detection/prevention tools and solutions for all capable devices. Host based intrusion/prevention solutions report centrally to be used for monitoring of anomalous traffic, exfiltration, and indicators of insider threat.
Discussion	Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capability. The information contained in one intrusion detection tool can be shared widely across the organization making the system-wide detection capability more robust and powerful.
Related Controls	None
References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (10) SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS

Control Selection Rationale	Encrypted tunnels are often used by insiders or malicious actors to extract information because the traffic payload cannot be easily inspected. Organizations should inspect encrypted traffic to ensure that the traffic is legitimate and not exfiltration of data.
Control Direction:	The organization should balance the need for encrypted traffic and inspection of the traffic. They should determine the best approach to mitigating the risks associated with encrypted traffic. Examples include choosing to limit encrypted traffic to only authorized encrypted connections and locations, encrypted traffic entering and leaving the environment with unknown or public sources, or destinations is decrypted and inspected to determine the appropriateness of use and unencrypt inbound traffic at known locations so it can be inspected and block all outbound unauthorized encrypted traffic.

Discussion	Organizations should balance the need for encrypting communications traffic to protect data confidentiality with the need for having visibility into such traffic from a monitoring perspective. Organizations can determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.
Related Controls	None
References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (11) SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Control Selection Rationale	Detecting anomalous traffic at the authorization boundary and at access control points inside the boundary provides the organization monitoring information for detecting malicious traffic and exfiltration from external and insider threats.
Control Direction:	The organization should monitor outbound and inbound traffic at the authorization boundary as well as strategic points inside the environment, such as boundary protection devices isolating the tiers (enclaves) to detect for anomalies, malicious traffic, or threats.
Discussion	Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.
Related Controls	None
References	OMB Circular A-130, NIST SP 800-61 Rev2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (13) SYSTEM MONITORING | ANALYZE TRAFFIC AND EVENT PATTERNS

Control Selection Rationale	Analyzing and profiling regular traffic and user action patterns provides a baseline that can be used to detect unusual activities, traffic, or events that could indicate a compromise of information or threat to the system.
Control Direction:	The organization should:
Item a	analyze communications traffic and event patterns for the system at the authorization boundary and at access control points inside the

	environment, such as boundary protection devices isolated the tiers (enclaves), to establish regular traffic patterns and actions.
Item b	They should continue to monitor traffic in these same locations and use the baselines as a comparison to detect for unusual traffic; and
Item c	configure detection monitoring tools with these baseline characteristics to alert on threshold values.
Discussion	Identifying and understanding common communications traffic and event patterns helps organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.
Related Controls	None
References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (18) SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION

Control Selection Rationale	Monitoring and analyzing outbound traffic for exfiltration protects the HVA system and information from potential compromise.
Control Direction:	The organization should monitor and inspect outbound communications traffic at the HVA authorization boundary and at strategic locations inside the boundary to detect covert exfiltration of information.
Discussion	Organization-defined HVA system interior points should include both subnetwork and subsystem information. Covert means that can be used to exfiltrate information include steganography.
Related Controls	None
References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (20) SYSTEM MONITORING | PRIVILEGED USERS

Control Selection Rationale	With privileged accounts permitted to make system level changes, enhanced tracking and monitoring of privileged user actions is necessary to provide the visibility into any potential malicious actions performed by these accounts.
Control Direction:	The organization should implement additional monitoring of privileged user account actions based on established policies. They should determine what additional monitoring attributes for privileged account

	are implemented based on risk assessment and potential impact to the environment. i.e., successful process execution, successful resource access, etc.
Discussion	Privileged users may have access to more HVA data, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to HVA systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure organizations can identify malicious activity at the earliest possible time and take appropriate actions.
Related Controls	AC-18
References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (22) SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES

Control Selection Rationale	Unauthorized network services and traffic can indicate a threat or compromise on the system. Monitoring and detecting for unauthorized network services is necessary to identify potential threats to the information and systems.
Control Direction:	The organization should:
Item a	define authorized network services and implement solutions to detect unauthorized network services on the network; and
Item b	create alerts when detected.
Discussion	Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services. Examples include peer-to-peer communications and Internet relay chat.
Related Controls	CM-7
References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-4 (23) SYSTEM MONITORING | HOST-BASED DEVICES

Control Selection Rationale	System-wide monitoring provides a greater view of threats against the HVA environment and allows for better correlation and analysis of incidents.
Control Direction:	The organization should implement individual host-based monitoring tools and solutions on capable devices within the HVA accreditation boundary.

Discussion	System components where host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.
Related Controls	AC-18, AC-19
References	OMB Circular A-130, NIST SP 800-61 Rev 2, NIST SP 800-92, NIST SP 800-137
CSF Function Mapping	Identify, Protect, Detect, Respond

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control Selection Rationale	Security alerts, advisories, and directives enable the organization to make risk-informed decisions or take actions to mitigate developing SR risks in a timely manner.
Control Direction:	The organization should:
Item a	receive HVA security alerts, advisories, and directives from external organizations on an ongoing basis;
Item b	generate internal HVA security alerts, advisories, and directives as deemed necessary;
Item c	disseminate HVA security alerts, advisories, and directives to the organization's HVA PMO staff and other key stakeholders; and
Item d	implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.
Discussion	CISA generates security alerts and advisories to maintain situational awareness throughout the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation if not implemented in a timely manner.
Related Controls	PM-15, RA-5, SI-2
References	NIST SP 800-161 v2
CSF Function Mapping	Identify, Respond

Supply Chain Risk Management (SR)

SR-4 (2) PROVENANCE | TRACK AND TRACE	
Control Selection Rationale	The organization can reduce HVA supply chain risks by tracking each HVA and HVA component (as applicable) from the origin. The organization can establish and maintain the HVA or HVA component's origin by creating and assigning unique identifiers for tracking through the supply chain.
Control Direction:	The organization should establish and maintain unique identification of the HVA for the purposes of tracking the HVA during development and transport through the supply chain.
Discussion	The HVA and HVA components may be labeled using serial numbers or tagged using radio-frequency identification tags. Labels and tags can help provide better visibility into the provenance of the HVA or HVA component. The HVA or HVA component may have more than one unique identifier and these identification methods should be sufficient to support a forensic investigation after a supply chain compromise or event.
Related Controls	IA-2, IA-8, PE-16, PL-2
References	NIST SP 800-161, NISTIR 7622
CSF Function Mapping	Identify, Protect

SR-4 (3) PROVENANCE | VALIDATE AS GENUINE AND NOT ALTERED	
Control Selection Rationale	HVA and HVA components face the risk of being altered as they traverse through the organization's supply chain. Ensuring the HVA or HVA component is genuine and unaltered upon delivery reduces the risk of maliciously altered software, hardware, or firmware being introduced into the organization's operational environment.
Control Direction:	The organization should employ controls and/or conduct testing to validate the HVA or HVA component received is genuine and has not been altered along the organization's supply chain.
Discussion	For many systems and system components, especially hardware, there are technical means to determine if the items are genuine or have been altered. Controls can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Organizations may leverage supplier and contractor processes for validating that a system or component is genuine and has not been altered, and for replacing a suspect system or component. Some indications of tampering may be visible and addressable before accepting delivery. When the HVA or HVA component is suspected of being altered or counterfeit, the supplier, contractor, or original equipment manufacturer may be able to replace the item or provide a

	forensic capability to determine the origin of the counterfeit or altered item.
Related Controls	AT-3, SR-9, SR-10, SR-11
References	NIST SP 800-161, NISTIR 7622
CSF Function Mapping	Identify, Protect, Detect

SR-5 (2) ACQUISITION STRATEGIES, TOOLS, AND METHODS | ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE

Control Selection Rationale	Organizations can discover evidence of tampering, intentional or unintentional vulnerabilities, and non-compliance with supply chain controls by assessing the HVA or HVA components prior to selection, acceptance, modification, and/or updates.
Control Direction:	The organization should assess the HVAs, HVA components, and HVA system services prior to selection, acceptance, modification of and/or updates to those assets.
Discussion	Evidence of tampering or vulnerabilities could include malicious code or processes, defective software, backdoors, and counterfeits. Assessments can include evaluations, design proposal reviews, visual or physical inspection, static and dynamic analyses, visual, x-ray, or magnetic particle inspections, simulations, white, gray, or black box testing, fuzz testing, stress testing, or penetration testing. Evidence generated during assessments should be documented for follow-on actions by organizations. The evidence generated during the organizational or independent assessments of supply chain elements may be used to improve supply chain processes and to inform the supply chain risk management process.
Related Controls	CA-8, RA-5, SA-11, SI-7, SR-9
References	NIST SP 800-30, NIST SP 800-161, NISTIR 7622
CSF Function Mapping	Detect

SR-9 TAMPER RESISTANCE AND DETECTION

Control Selection Rationale	Anti-tamper capabilities increase the resiliency of the HVA, HVA components and HVA services against tampering attempts and help detect instances of tampering.
Control Direction:	The organization should implement tamper protection capabilities for the HVA, HVA components, and HVA services.
Discussion	Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many

	threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.
Related Controls	PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11
References	N/A
CSF Function Mapping	Protect, Detect

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS	
Control Selection Rationale	Periodic HVA and HVA component inspections can help agencies detect instances of tampering.
Control Direction:	The organization should inspect the HVA and/or HVA components to detect tampering at random, annually, or upon detection of potential indicators of tampering.
Discussion	Inspection of the HVA or HVA components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components taken out of organization-controlled areas. Indications of a need for inspection include when individuals return from travel to high-risk locations.
Related Controls	AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11
References	N/A
CSF Function Mapping	Protect, Detect

Enterprise Controls

The organization's HVA often relies on the support systems and network infrastructure that comprise the organization's broader enterprise architecture. The HVA's dependency on the enterprise should be considered when identifying risks and corresponding controls for the HVA. For example, an underdeveloped enterprise-wide contingency plan may result in significant downtimes for support systems or architecture that is critical to the functionality or operation of the HVA. Organizations should account for HVA dependencies on the enterprise in the process of securing their HVAs.

The controls in this section are recommended for implementation at the enterprise level in order to further secure the HVA.

Audit and Accountability (AU)

AU-6 (3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES	
Control Selection Rationale	The organization can improve situational awareness and enterprise risk management of HVA information and systems by correlating audit records across organizational-wide audit repositories.
Control Direction:	The organization should manage enterprise risk by correlating audit logs and events from all organizational systems to form a single risk view of the enterprise.
Discussion	Audit data collected at the system level (Tier 3) should be aggregated with audit data from other systems to form a system-level enterprise view of audit records. Audit information must be protected at a level congruent with the highest level of information it contains (AU-9). Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and support cross-organization awareness. Organization-wide situational awareness includes awareness across all three levels of risk management and support cross-organization awareness.
Related Controls	AU-9, AU-12, IR-4
References	OMB Circular A-130, NIST SP 800-137, NIST SP 800-37 Rev 1 and Rev 2
CSF Function Mapping	Identify, Detect, Respond

AU-6 (4) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS	
Control Selection Rationale	The organization can improve situational awareness and reactions to incidents by reviewing and analyzing audit records and events from all repositories.
Control Direction:	The organization should provide capabilities that allow for centrally reviewing and analyzing audit records and events for all components.
Discussion	Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.
Related Controls	AU-2, AU-12
References	OMB Circular A-130, NIST SP 800-137
CSF Function Mapping	Identify, Detect, Respond

AU-6 (5) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS	
Control Selection Rationale	The organization can identify threats, inappropriate actions, or unusual activities by correlating audit record information with vulnerability, performance data, and/or system monitoring information provides
Control Direction:	The organization should integrate audit records (from sources including vulnerability scanning, performance data, and system monitoring) into a central repository for analysis, parsing, and correlation of events to detect threats, and inappropriate or unusual activities.
Discussion	Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial of service attacks or other types of attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.
Related Controls	AU-12, IR-4
References	OMB Circular A-130, NIST SP 800-137
CSF Function Mapping	Identify, Detect, Respond

Contingency Planning (CP)

CP-2 CONTINGENCY PLAN	
Control Selection Rationale	A robust HVA contingency plan enables the organization to rapidly resume HVA operations that support essential organizational missions and business functions after an incident.
Control Direction:	The organization should:
Item a	develop a contingency plan for organizational systems to include HVAs

	that: identifies essential missions and business functions and associated contingency requirements, provides recovery objectives, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information, addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; addresses eventual, full system restoration without deterioration of the controls originally planned and implemented, and is reviewed and approved by the agency CISO;
Item b	distribute copies of the contingency plan to key agency cybersecurity, risk, operational, and technical staff members who are direct or indirect stakeholders, as outlined in the contingency plan's communications plan;
Item c	develop the contingency plan's communications plan that outlines how the contingency plan will be communicated to the organization and HVA stakeholders, as determined in 'Item b' above;
Item d	ensure contingency planning activities are included with incident handling activities;
Item d	review the contingency plan for the HVA at least biannually;
Item e	update the contingency plan to address changes to the organization, system, or environment of operation and annotate problems encountered during contingency plan implementation, execution, or testing;
Item f	communicate contingency plan changes to at least all personnel who have received a copy of the contingency plan;
Item g	incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
Item h	protect the contingency plan from unauthorized disclosure and modification.
Discussion	Contingency planning for systems to include HVAs is part of the organization's overall program for achieving continuity of operations for organizational missions and business functions. Contingency planning addresses HVA restoration and implementation of alternative mission or business processes if the HVA is compromised or breached. Contingency planning should be considered throughout the HVA system development life cycle and is a fundamental part of the system design. Contingency plans reflect the degree of restoration required for organizational HVAs since not all systems need to fully recover to achieve the level of continuity of operations desired. HVA recovery objectives should reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls	CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12
References	NIST SP 800-34, NISTIR 8179
CSF Function Mapping	Protect, Detect, Respond, Recover

CP-8 (5) TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING	
Control Selection Rationale	Alternate telecom connections can sit idle and untested for extended periods of time that may result in failure when they are needed causing a loss of availability of the systems.
Control Direction:	The organization should test alternate telecommunication services at least every 6 months.
Discussion	Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure there is no degradation in organizational missions or functions.
Related Controls	CP-3
References	OMB Circular A-130, NIST SP 800-61 Rev 2
CSF Function Mapping	Identify, Protect

Incident Response (IR)

IR-4 (4) INCIDENT HANDLING | INFORMATION CORRELATION	
Control Selection Rationale	The organization can improve threat identification timeliness by correlating incident information across the enterprise.
Control Direction:	The organization should correlate incident information and individual incident responses across the enterprise to achieve an organization-wide perspective on incident awareness and response.
Discussion	Correlation information must be protected at a level congruent with the highest level of information it contains (AU-9). Sometimes a threat event, for example, a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Related Controls	AU-9
References	OMB Circular A-130, NIST SP 800-61 Rev 2
CSF Function Mapping	Detect, Respond, Recover

Program Management (PM)

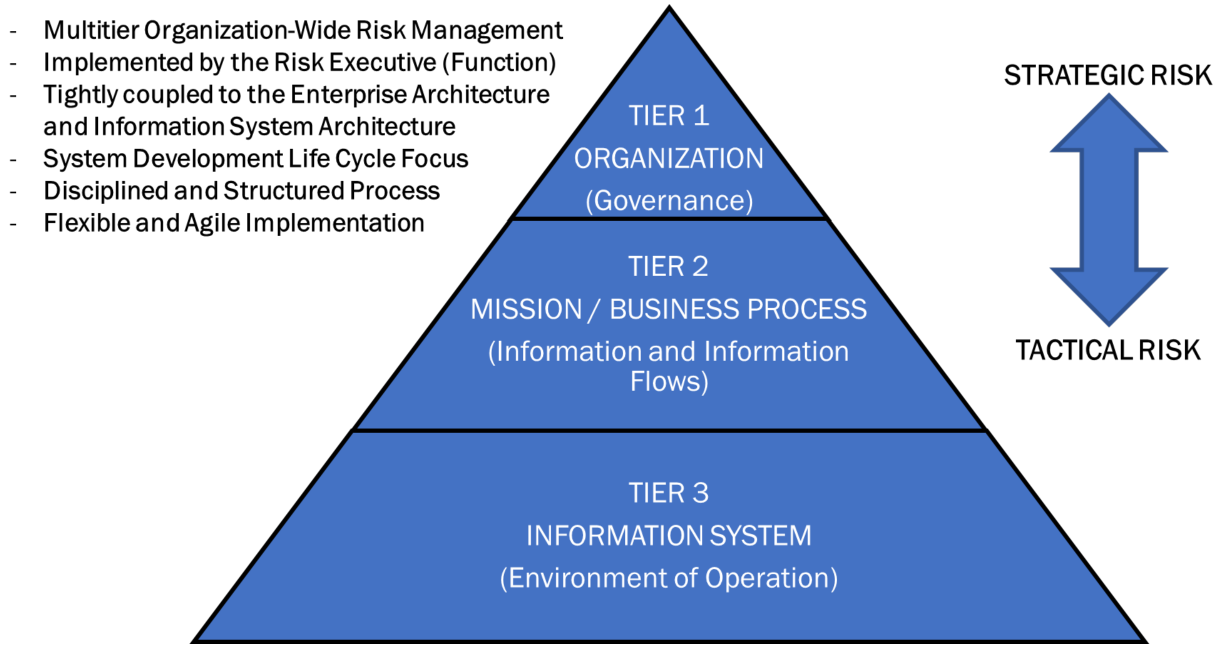
PM-7 ENTERPRISE ARCHITECTURE	
Control Selection Rationale	The organization can reduce the risk of HVA compromise from adjacent systems through proper segmentation, regular security updates, and security/privacy controls in place on adjacent systems.
Control Direction:	The organization should develop and maintain an EA with consideration for information security, privacy, and the resulting risk to the organization's HVA and HVA operations.
Discussion	The dependency of the HVAs on the enterprise mandates the integration of security requirements and controls into the Enterprise Architecture (EA) to ensure HVAs are adequately protected by the enterprise to ensure the critical business functions and mission of the organization. The enterprise is considered a large and complex system, or system of systems. The EA should align business and technology resources to achieve strategic outcomes. agencies should develop an EA that describes the baseline architecture, target architecture, and transition plan to get to the target architecture while considering organizational risk management, effective security control implementation, and if necessary, privacy strategies. The EA should be implemented, enforced, and executed at levels 1 and 2: Organization (level 1), mission/business (level 2) but must facilitate and support the functions and solutions at the System or component level (level 3). The EA should also incorporate agency plans for significant upgrades or replacements of legacy applications, systems, or solutions that are too costly to operate, maintain, and secure. The EA should include plans for disposition of applications, systems, or solutions when no longer effectively support missions or business functions as well as strategies for interacting and connecting to external systems and environments (cloud, hosting providers, other government entities, contractor facilities. As organizations develop plans for transitioning from current operations to the desired future states, opportunities to further secure the enterprise in support of HVAs should be considered along with reduced waste and duplication, migration to shared services, closing of performance gaps, and modernization.
Related Controls	AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17
References	OMB Circular A-130, NIST SP 800-37

CSF Function Mapping	Identify

PM-9 RISK MANAGEMENT STRATEGY

Control Selection Rationale	The organization can reduce risks posed to the enterprise and to the HVA by developing and implementing a comprehensive risk management strategy.
Control Direction:	The organization should:
Item a	develop a comprehensive strategy to manage security risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems, as well as privacy risks to individuals resulting from the authorized processing of personally identifiable information;
Item b	implement the risk management strategy consistently across the organization;
Item c	account for HVAs in the development of the enterprise-wide risk management strategy to ensure changes to the enterprise do not create unknown or unacceptable risks to the HVA; and
Item d	review and update the risk management strategy at least annually or as required, to address organizational changes.
Discussion	The enterprise risk management strategy includes a process to evaluate all risks to HVA information and mission critical services. Per OMB M-19-03: “HVA risk assessments should incorporate operational, business, mission, and continuity considerations.” Organizations should develop an enterprise wide risk management strategy that includes is holistic and integrated into the three-levels of the organization. Figure 4 illustrates the three-level approach to risk management that addresses risk-related concerns at the enterprise level, the mission/business process level, and the HVA system level. At a minimum, organizations should: Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework, establish a risk management strategy for the organization that includes a determination of risk tolerance, identify the missions, business functions, and mission/business processes the HVA system(s) will support, identify HVA stakeholders who have a security interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system, identify assets that require protection, conduct an initial risk assessment of HVA assets and update the risk assessment on an ongoing basis, define the HVA protection needs and HVA security requirements, and determine the placement of the HVA within the EA. (PM-7)
Related Controls	AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1,

	MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2
References	OMB Circular A-130, NIST SP 800-37 R1, NIST SP 800-160, NIST SP 800-39.
CSF Function Mapping	Identify



- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to the Enterprise Architecture and Information System Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TIER 3
INFORMATION SYSTEM
(Environment of Operation)
STRATEGIC RISK
TACTICAL RISK

Figure 4. Enterprise Risk Management Approach

PM-10 AUTHORIZATION PROCESS

Control Selection Rationale	The organization can identify and characterize risks to the HVA through the system authorization process.
Control Direction:	The organization should:
Item a	manage the security and privacy state of the HVA and other organizational systems and the environments in which those systems operate through authorization processes;
Item b	designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
Item c	integrate the authorization processes into an organization-wide risk management program.
Discussion	The organization may adopt an enterprise-wide perspective and approach to both the risks posed by the HVA and the related organizational responsibilities as part of the authorization process. The organization should follow a sound, documented and well-understood authorization approach that meets the protection needs of all stakeholders and is recommended for HVAs. OA is a time-driven or event-driven authorization process whereby the AO is provided with the necessary and sufficient information regarding the security and privacy state of the HVA to determine whether the mission or business risk of continued HVA operation is acceptable.[22] OA requires that agencies have a fully implemented ISCM program as defined in NIST SP 800-137. agencies should leverage CDM tools and methods to automate collection, review, and alerting requirements of OA where possible.
Related Controls	CA-6, CA-7, PL-2
References	CA-6, CA-7, PM-9, CDM: CDM and the Risk Management Framework
CSF Function Mapping	Identify

PM-12 INSIDER THREAT PROGRAM

Control Selection Rationale	The organization can institute an Insider Threat Program to mitigate risks posed by malicious insiders.
Control Direction:	The organization should implement an insider threat program that accounts for potential impacts to the HVA.
Discussion	Given the sensitivity of the HVA, organizations develop and implement an insider threat program in accordance with ODNI National Insider

[22] Dempsey et. al. "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", NIST SP 800-137, September 2011, https://csrc.nist.gov/publications/detail/sp/800-137/final

	Threat Task Force's "National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs." A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the insider threat program. The program is authorized by policy and outlines the processes executed by the organization to detect and respond to insider threats through technical and non-technical means. Organizations implement controls and capabilities to prevent malicious insider threats actions (e.g., DLP, monitoring, access controls, etc.) and provide insider threat training to all employees and contractors.
Related Controls	AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14
References	OMB Circular A-130, National Insider Threat Policy and the Minimum Standards, ODNI
CSF Function Mapping	Identify

Risk Assessment (RA)

RA-3 RISK ASSESSMENT	
Control Selection Rationale	The organization can make risk-informed decisions regarding the HVA by assessing risk at the HVA and other levels (organizational and mission/business process level).
Control Direction:	The organization should:
Item a	conduct a risk assessment, including: the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information, and the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
Item b	integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
Item c	document risk assessment results in the HVA system security plan, HVA risk assessment report, or other agency-defined HVA risk assessment document;
Item d	review risk assessment results at least biannually;
Item e	disseminate risk assessment results to the HVA system owners and staff; and

Item f	update the risk assessment at least annually or when there are significant changes to the information system or environment of operation (including identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
Discussion	Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of systems. Risk assessments also consider risk from external parties, including individuals accessing organizational systems; contractors operating systems on behalf of the organization; service providers; and outsourcing entities.
Related Controls	CA-3, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12
References	OMB Circular A-130, NIST SP 800-30, NIST SP 800-39, NIST SP 800-161, NISTIR 8023, NISTIR 8062
CSF Function Mapping	Identify, Protect, Detect, Respond, Recover

System and Information Integrity (SI)

SI-4 (16) SYSTEM MONITORING | CORRELATE MONITORING INFORMATION	
Control Selection Rationale	The organization can establish comprehensive situational awareness the enterprise security and potential threats and attacks to the HVA by correlating monitoring information enterprise-wide.
Control Direction:	The organization should correlate information from monitoring tools and mechanisms employed throughout the enterprise.
Discussion	Organizations should correlate monitoring information from enterprise monitoring tools and mechanisms such as, but not limited to antivirus monitoring, Intrusion Detection System, Intrusion Prevention System, logging, etc. Organizations should protect this information at the level commensurate with the highest level of information contained within.
Related Controls	AU-6
References	OMB Circular A-130
CSF Function Mapping	Identify, Protect, Detect, Respond, Recover

Supply Chain Risk Management (SR)

SR-6 SUPPLIER REVIEWS	
Control Selection Rationale	The organization can reduce the risk of acquiring HVAs, HVA components or services through compromised or malicious vendors by conducting supplier and/or contractor reviews.
Control Direction:	If the organization intends to have a continued relationship with providers for the HVA system updates/component acquisition, the organization should review the supply chain-related risks associated with suppliers, contractors, the HVA, HVA components, or HVA system services the suppliers and/or contractors provide:
Item a	before a one-time purchase of the HVA, component, or service;
Item b	at least biannually for regularly purchased or long-term purchases of an, component, or service; and
Item c	if possible, after a major breach or incident occurs with a supplier or contractor within the organization's supply chain.
Discussion	A review of supplier risk includes security processes, foreign ownership, control or influence, and the ability of the supplier to effectively assess any subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate to share review results with other organizations in accordance with any applicable agreements or contracts.
Related Controls	SR-3, SR-5
References	FIPS 140-3, FIPS 180-4, FIPS 186-4, FIPS 202, NIST SP 800-30, NIST SP 800-161, NISTIR 7622
CSF Function Mapping	Identify, Protect

Appendix 1: Acronym List

Acronym	Term
5G	Fifth Generation
ABAC	Attribute-Based Access Control
AC	Access Control
AI	Artificial Intelligence
ANSI	American National Standards Institute
AO	Authorizing Official
AT	Awareness and Training
ATO	Authorization to Operate
AU	Audit and Accountability
BOD	Binding Operational Directive
CA	Security Assessment and Authorization
CAC	Common Access Card
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CM	Configuration Management
COTS	Commercial off-the-Shelf
CP	Contingency Planning
CSF	Cybersecurity Framework
DAC	Discretionary Access Control
DAR	Data-at-Rest
DHS	Department of Homeland Security
DME	Development Modernization Enhancement
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
EA	Enterprise Architecture
EAP	Extensible Authentication Protocol
EO	Executive Order
FAR	Federal Acquisition Regulation
FCEE	Federal Civilian Enterprise Essential
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GOTS	Government-off-the-Shelf
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVA	High Value Asset
IA	Identification and Authentication
IaaS	Infrastructure as a Service
ID	Identification
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol

IPS	Intrusion Prevention System
IR	Incident Response
IR	Internal Report
ISA	Interconnection Security Agreements
ISCM	Information Security Continuous Monitoring
IT	Information Technology
MA	Maintenance
MAC	Mandatory Access Control
MAC	Media Access Control
MOU/A	Memorandum of Understanding/Agreement
MP	Media Protection
NCCoE	The National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NITP	National Insider Threat Policy
NSS	National Security Systems
NVD	National Vulnerability Database
OA	Ongoing Authorization
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OS	Operating System
OVAL	Open Vulnerability Assessment Language
PaaS	Platform as a Service
PPD	Presidential Policy Directive
PE	Physical and Environmental Protection
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
PMEF	Primary Mission Essential Functions
PMO	Program Management Office
POA&M	Plan of Action and Milestones
PPBE	Planning, Programming, Budgeting and Execution
PS	Personnel Security
PT	Personally Identifiable Information Processing and Transparency
RA	Risk Assessment
RBAC	Role-Based Access Control
REV	Revision
SA	System Administrator
SA	System and Services Acquisition
SaaS	Software as a Service
SC	System and Communications Protection
SCAP	Security Content Automation Protocol
SI	System and Information Integrity
SP	Special Publication
SR	Supply Chain Risk Management
SSL	Secure Sockets Layer

TCP	Transmission Control Protocol
TLS	Transport Layer Security
US-CERT	United States Computer Emergency Readiness Team
V	Version
VPN	Virtual Private Network

Appendix 2: High Value Asset Controls

The following table contains the list of recommended security controls included within this HVA Control Overlay. More information about these controls can be found within NIST SP 800-53 Rev 5.

High Value Asset Controls
Access Control (AC)
AC-2 Account Management
AC-2 (2) Account Management | Automated Temporary and Emergency Account Management
AC-3 Access Enforcement
AC-3 (9) Access Enforcement | Controlled Release
AC-4 Information Flow Enforcement
AC-5 Separation of Duties
AC-6 Least Privilege
AC-6 (5) Least Privilege | Privileged Accounts
AC-6(7) Least Privilege | Review of User Privileges
AC-17 Remote Access
AC-17 (2) Remote Access | Protection of Confidentiality and Integrity Using Encryption
AC-20 Use of External Systems
Audit and Accountability (AU)
AU-2 Event Logging
AU-6 Audit Record Review, Analysis, and Reporting
AU-9 Protection of Audit Information
AU-9 (2) Protection of Audit Information | Store on Separate Physical Systems or Components
AU-9 (3) Protection of Audit Information | Cryptographic Protection
AU-9 (5) Protection of Audit Information | Dual Authorization
AU-9 (6) Protection of Audit Information | Read-Only Access
AU-10 Non-Repudiation
AU-16 Cross-Organizational Audit Logging
Awareness and Training (AT)
AT-2 (1) Awareness Training | Practical Exercises
Assessment, Authorization, and Monitoring (CA)
CA-3 Information Exchange
CA-5 Plan of Action and Milestones
CA-6 Authorization
CA-6 (1) Authorization | Joint Authorization-Intra-Organization
CA-7 Continuous Monitoring
CA-7 (3) Continuous Monitoring | Trend Analysis
CA-9 Internal System Connections
Configuration Management (CM)
CM-2 Baseline Configuration
CM-3 (2) Configuration Change Control | Testing, Validation, and Documentation of Changes
CM-3 (7) Configuration Change Control | Review System Changes
CM-4 (1) Impact Analyses | Separate Test Environments
CM-6 Configuration Settings

CM-6 (2) Configuration Settings | Respond to Unauthorized Changes
CM-7 (1) Least Functionality | Periodic Review
CM-8 System Component Inventory
Contingency Planning (CP)
CP-4 Contingency Plan Testing
CP-7 Alternate Processing Site
CP-7 (3) Alternate Processing Site | Priority of Service
CP-9 (1) System Backup | Testing for Reliability and Integrity
CP-10 (4) System Recovery and Reconstitution | Restore within Time-Period
Identification and Authentication (IA)
IA-2 Identification and Authentication (Organizational Users)
IA-2 (1) Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts
IA-2 (2) Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts
IA-2 (12) Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials
IA-3 Device Identification and Authentication
IA-5 Authenticator Management
IA-5 (1) Authenticator Management | Password-Based Authentication
Incident Response (IR)
IR-4 (2) Incident Handling | Dynamic Reconfiguration
IR-4 (8) Incident Handling | Correlation with External Organizations
IR-4 (10) Incident Handing | Supply Chain Coordination
IR-5 Incident Monitoring
Media Protection (MP)
MP-6 Media Sanitization
MP-6 (8) Media Sanitization | Remote Purging or Wiping of Information
Physical and Environmental Protection (PE)
PE-3 Physical Access Control
PE-3 (1) Physical Access Control | System Access
Planning (PL)
PL-2 System Security and Privacy Plans
PL-8 Security and Privacy Architectures
PL-8 (1) Security and Privacy Architectures | Defense-in-Depth
PL-10 Baseline Selection
Personally Identifiable Information Processing and Transparency (PT)
PT-3 (1) Personally Identifiable Information Processing Purposes | Data Tagging
PT-3 (2) Personally Identifiable Information Processing Purposes | Automation
Risk Assessment (RA)
RA-2 Security Categorization
RA-3 (1) Risk Assessment | Supply Chain Risk Assessment

RA-5 Vulnerability Monitoring and Scanning
RA-5 (6) Vulnerability Monitoring and Scanning | Automated Trend Analysis
RA-5 (10) Vulnerability Monitoring and Scanning | Correlate Scanning Information
System and Services Acquisition (SA)
SA-4 Acquisition Process
SA-9 External System Services
SA-11 Developer Testing and Evaluation
SA-11 (1) Developer Testing and Evaluation | Static Code Analysis
SA-11 (2) Developer Testing and Evaluation | Threat Modeling and Vulnerability Analysis
SA-11 (4) Developer Testing and Evaluation | Manual Code Reviews
SA-11 (5) Developer Testing and Evaluation | Penetration Testing
SA-11 (8) Developer Testing and Evaluation | Dynamic Code Analysis
System and Communications Protection (SC)
SC-3 Security Function Isolation
SC-3 (2) Security Function Isolation | Access and Flow Control Functions
SC-5 Denial of Service Protection
SC-5 (1) Denial of Service Protection | Restrict Ability to Attack other Systems
SC-5 (2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
SC-5 (3) Denial of Service Protection | Detection and Monitoring
SC-7 Boundary Protection
SC-7 (3) Boundary Protection | Access Points
SC-7 (5) Boundary Protection | Deny by Default - Allow by Exception
SC-7 (10) Boundary Protection | Prevent Exfiltration
SC-7 (11) Boundary Protection | Restrict Incoming Communications Traffic
SC-7 (12) Boundary Protection | Host-Based Protection
SC-7 (14) Boundary Protection | Protection Against Unauthorized Physical Connections
SC-7 (17) Boundary Protection | Automated Enforcement of Protocol Formats
SC-7 (21) Boundary Protection | Isolation of System Components
SC-7 (22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains
SC-8 Transmission Confidentiality and Integrity
SC-18 (4) Mobile Code | Prevent Automatic Execution
SC-28 Protection of Information at Rest
SC-28 (1) Protection of Information at Rest | Cryptographic Protection
System and Information Integrity (SI)
SI-2 Flaw Remediation
SI-3 Malicious Code Protection
SI-4 System Monitoring
SI-4 (1) System Monitoring | System Wide Intrusion Detection System
SI-4 (10) System Monitoring | Visibility of Encrypted Communications
SI-4 (11) System Monitoring | Analyze Communications Traffic Anomalies
SI-4 (13) System Monitoring | Analyze Traffic and Event Patterns
SI-4 (18) System Monitoring | Analyze Traffic and Covert Exfiltration
SI-4 (20) System Monitoring | Privileged Users
SI-4 (22) System Monitoring | Unauthorized Network Services
SI-4 (23) System Monitoring | Host-Based Devices

SI-5 Security Alerts, Advisories, and Directives
Supply Chain Risk Management (SR)
SR-4 (2) Provenance | Track and Trace
SR-4 (3) Provenance | Validate as Genuine and Not Altered
SR-5 (2) Acquisition Strategies, Tools, and Methods, Control Enhancement | Assessments Prior to Selection, Acceptance, Modification, or Update
SR-9 Tamper Resistance and Detection
SR-10 Inspection of Systems or Components
Enterprise Controls
Audit and Accountability (AU)
AU-6 (3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories
AU-6 (4) Audit Record Review, Analysis, and Reporting | Central Review and Analysis
AU-6 (5) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records
Contingency Planning (CP)
CP-2 Contingency Plan
CP-8(5) Telecommunications Services | Alternate Telecommunication Service Testing
Incident Response (IR)
IR-4 (4) Incident Handling | Information Correlation
Program Management (PM)
PM-7 Enterprise Architecture
PM-9 Risk Management Strategy
PM-10 Authorization Process
PM-12 Insider Threat Program
Risk Assessment (RA)
RA-3 Risk Assessment
System and Information Integrity (SI)
SI-4 (16) System Monitoring | Correlate Monitoring Information
Supply Chain Risk Management (SR)
SR-6 Supplier Reviews

Appendix 3: NIST Cybersecurity Framework Crosswalk

The following table crosswalks the Overlay's security controls to the NIST CSF's five functions: Identify, Protect, Detect, Respond, and Recover. Multiple functions may be associated with a single control. An 'X' indicates that the function applies to the corresponding control.

Control	NIST Cybersecurity Framework Function				
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
AC-2		X	X		
AC-2 (2)		X	X		
AC-3		X			
AC-3 (9)		X			
AC-4	X	X			
AC-5		X			
AC-6		X			
AC-6 (5)		X			
AC-6 (7)		X			
AC-17		X			
AC-17 (2)		X			
AC-20	X	X			
AU-2	X				
AU-6			X	X	
AU-9		X			
AU-9 (2)		X			
AU-9 (3)		X			
AU-9 (5)		X			
AU-9 (6)		X			
AU-10	X				
AU-16	X				
AT-2 (1)		X			
CA-3	X		X		
CA-5	X	X	X		
CA-6	X				
CA-6 (1)	X				
CA-7		X	X	X	
CA-7 (3)	X	X			
CA-9		X			
CM-2		X	X		
CM-3 (2)		X	X		
CM-3 (7)		X	X		
CM-4 (1)		X			
CM-6	X	X			

CM-6 (2)			X	X	
CM-7 (1)		X			
CM-8	X	X	X		
CP-4		X			
CP-7		X			X
CP-7 (3)		X			X
CP-9 (1)					X
CP-10 (4)					X
IA-2		X			
IA-2 (1)		X			
IA-2 (2)		X			
IA-2 (12)		X			
IA-3		X			
IA-5		X			
IA-5 (1)		X			
IR-4 (2)			X	X	X
IR-4 (8)			X	X	X
IR-4 (10)			X	X	X
IR-5			X	X	
MP-6		X			
MP-6 (8)		X			
PE-3		X	X		
PE-3 (1)		X	X		
PL-2		X	X		
PL-8	X	X			
PL-8 (1)	X	X			
PL-10	X	X			
PT-3 (1)	X				
PT-3 (2)	X				
RA-2	X				
RA-3 (1)	X	X	X	X	
RA-5	X	X	X	X	
RA-5 (6)	X	X	X	X	
RA-5 (10)	X	X	X	X	
SA-4		X	X		
SA-9	X	X	X		
SA-11	X	X			
SA-11 (1)	X	X			
SA-11 (2)	X	X			
SA-11 (4)	X	X			
SA-11 (5)	X	X			

SA-11 (8)	X	X			
SC-3	X				
SC-3 (2)	X				
SC-5	X	X	X		
SC-5 (1)	X	X	X		
SC-5 (2)	X	X	X		
SC-5 (3)	X	X	X		
SC-7		X	X		
SC-7 (3)	X	X	X	X	
SC-7 (5)	X	X	X	X	
SC-7 (10)		X	X		
SC-7 (11)		X	X		
SC-7 (12)		X	X		
SC-7 (14)		X	X		
SC-7 (17)		X	X		
SC-7 (21)		X	X		
SC-7 (22)		X	X		
SC-8		X			
SC-18 (4)			X		
SC-28		X			
SC-28 (1)		X			
SI-2	X	X			
SI-3	X				
SI-4	X	X	X	X	
SI-4 (1)	X	X	X	X	
SI-4 (10)	X	X	X	X	
SI-4 (11)	X	X	X	X	
SI-4 (13)	X	X	X	X	
SI-4 (18)	X	X	X	X	
SI-4 (20)	X	X	X	X	
SI-4 (22)	X	X	X	X	
SI-4 (23)	X	X	X	X	
SI-5	X			X	
SR-4 (2)	X	X			
SR-4 (3)	X	X	X		
SR-5 (2)			X		
SR-9		X	X		
SR-10		X	X		
AU-6 (3)	X		X	X	
AU-6 (4)	X		X	X	
AU-6 (5)	X		X	X	

CP-2		X	X	X	X
CP-8 (5)	X	X			
IR-4 (4)			X	X	X
PM-7	X				
PM-9	X				
PM-10	X				
PM-12	X				
RA-3	X	X	X	X	X
SI-4 (16)	X	X	X	X	X
SR-6	X	X			

Additional References

The Clinger-Cohen Act of 1996, 40 U.S.C. § 1401, Pub. L. No. 104-106 (1996).

Committee on National Security Systems (CNSS). 2014. *Security Categorization and Security Control Selection for National Security Systems.* Instruction 1253.

Continuous Diagnostics and Mitigation. 2016. *CDM and the Risk Management Framework*. CISA. https://www.us-cert.gov/sites/default/files/cdm_files/LCE-2_MeetingSummary.PDF.

Cybersecurity and Infrastructure Security Agency (CISA). 2019. *Vulnerability Remediation Requirements for Internet-Accessible Systems.* Binding Operational Directive (BOD) 19-02. https://cyber.dhs.gov/bod/19-02/

Bartock, Mike, Jeff Cichonski, and Murugiah Souppaya. 2020. *Preparing a Secure Evolution to 5G.* Project Description, National Institute for Standards and Technology.

Boeckl, Kaitlin, Michael Fagan, William Fisher, Naomi Lefkovitz, Katerina Megas, Ellen Nadeau, Ben Piccarreta, Danna Gabel O'Rourke, and Karen Scarfone. 2019. "Considerations for Managing Internet of Things (IoT)." Interagency/Internal Report 8228, National Institute of Standards and Technology.

Boyens, Jon, Celia Paulsen, Rama Moorthy, and Nadya Bartol. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* Special Publication 800-161, National Institute of Standards and Technology.

Dempsey, Kelley, Nirali Chawla, L. Johnson, Ronald Johnston, Alicia Jones, Angela Orebaugh, Matthew Scholl, and Kevin Stine. 2011. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* Special Publication 800-137, National Institute of Standards and Technology.

Fagan, Michael, Katerina Megas, Karen Scarfone, and Matthew Smith. 2020. *Recommendations for IoT Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft).* Interagency/Internal Report 8259, National Institute of Standards and Technology.

Federal Agency Responsibilities, 44 U.S.C. § 3506 (2012).

Federal Information Security Management Act, Pub. L. No. 107-347, Title III (2014).

Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014).

Federal Records Act, 44 U.S.C. §3301, Pub. L. No. 90–620 (1950).

Frankel, Sheila, Karen Kent, Ryan Lewkowski, Angela Orebaugh, Ronald Ritchey, and Steven Sharma. 2005. *Guide to IPsec VPNs.* Special Publication 800-77, National Institute of Standards and Technology.

Frankel, Sheila, Paul Hoffman, Angela Orebaugh, and R. Park. 2008. *Guide to SSL VPNs.* Special Publication 800-113, National Institute of Standards and Technology.

Grance, Tim, Joan Hash, Steven Peck, Jonathan Smith, and Karen Korow-Diks. 2002. *Security Guide for Interconnecting Information Technology Systems.* Special Publication 800-47, National Institute of Standards and Technology.

Grassi, Paul, Michael Garcia, and James Fenton. 2017. *Digital Identity Guidelines.* Special Publication 800-63-3, National Institute of Standards and Technology.

Herring, MJ, and KD Willett. "Active Cyber Defense: A Vision for Real-Time Cyber Defense." *Journal of Information Warfare*, vol. 13, no. 2, 2014, pp. 46–55. *JSTOR*, www.jstor.org/stable/26487121. Accessed 14 Dec. 2020.

Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004.

Hu, Vincent, David Ferraiolo, Richard Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. 2014. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations.* Special Publication 800-162, National Institute of Standards and Technology.

Jansen, Wayne, and Tim Grance. 2011. *Guidelines on Security and Privacy in Public Cloud Computing.* Special Publication 800-144. National Institute of Standards and Technology.

Johnson, Christopher, Mark Badger, David Waltermire, Julie Snyder, and Clem Skorupka. 2016. *Guide to Cyber Threat Information Sharing.* Special Publication 800-150, National Institute of Standards and Technology.

Joint Task Force. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* Special Publication 800-37, Revision 2, National Institute of Standards and Technology.

Joint Task Force. 2020. *Security and Privacy Controls for Information Systems and Organizations (Final).* Special Publication 800-53 Revision 5, National Institute of Standards and Technology.

Joint Task Force Transformation Initiative. 2012. *Guide for Conducting Risk Assessments.* Special Publication 800-30 Revision 1, National Institute of Standards and Technology.

Kent, Karen, and Murugiah Souppaya. 2006. *Guide to Computer Security Log Management.* Special Publication 800-92, National Institute of Standards and Technology.

Mell, Peter, and Tim Grance. 2011. *The NIST Definition of Cloud Computing.* Special Publication 800-145, National Institute of Standards and Technology.

National Institute of Standards and Technology. 2020. "Control Baselines for Information Systems and Organizations." Special Publication 800-53B.

National Institute of Standards and Technology. 2006. "Personal Identity Verification (PIV) of Federal Employees and Contractors." Federal Information Processing Standards Publication 201-1.

National Institute of Standards and Technology. 2001. "Security Requirements for Cryptographic Modules." Federal Information Processing Standards Publication 140-2, National Institute for

Standards and Technology.

National Institute of Standards and Technology. 2004. "Standards for Security Categorization of Federal Information and Information Systems." Federal Information Processing Standards Publication 199.

National Institute of Standards and Technology. 2019. *What is 5G?* June 12. Accessed 2020. https://www.nist.gov/topics/advanced-communications/what-5g.

National Institute of Standards and Technology. 2018. “Framework for Improving Critical Infrastructure Cybersecurity”. Cybersecurity Framework.

Office of Director of National Intelligence. 2011. *Collection and Sharing of Audit Data.* Intelligence Community Standard 500-27.

Office of Director of National Intelligence. 2011. *Use of Audit Data for Insider Threat Detection.* Intelligence Community Standard 700-2.

Office of Management and Budget. 2011. "Continued Implementation of HSPD-12 Policy for Common Identification Standard for Federal Employees and Contractors." *Memorandum 11-11.*

Office of Management and Budget. 2016. " Managing Information as a Strategic Resource." *OMB Circular A-130.*

Office of Management and Budget Memorandum. 2013. "Enhancing the Security of Federal Information and Information Systems." *Memorandum 14-03.*

Office of Management and Budget. 2018. "Strengthening the Cybersecurity of Federal agencies by Enhancing the High Value Asset." *Memorandum 19-03.*

Office of Personnel Management. 2012. *Designation of Public Trust Positions and Investigative Requirements.* Title 5 *Code of Federal Regulations,* Pt. 731 Section 106.

Ross, Ron, Michael McEvilley, and Janet Oren. 2016. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* Special Publication 800-160, National Institute of Standards and Technology.

Souppaya, Murugiah, and Karen Scarfone. 2016. *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.* Special Publication 46 Revision 2, National Institute of Standards and Technology.

Stine, Kevin, Richard Kissel, William Barker, Jim Fahlsing, and Jessica Gulick. 2008. *Guide for Mapping Types of Information and Information Systems to Security Categories.* Special Publication 800-60 Volume 2 Revision 1, National Institute of Standards and Technology.

Swanson, Marianne, Joan Hash, and Pauline Bowen. 2006. *Guide for Developing Security Plans for Federal Systems.* Special Publication 800-18 Revision 1, National Institute of Standards and Technology.

Swanson, Marianne, Pauline Bowen, Amy Phillips, Dean Gallup, and David Lynes. 2010. *Contingency*

Planning Guide for Federal Information Systems. Special Publication 800-34, Revision 1, National Institute of Standards and Technology.

The Office of the Director of National Intelligence (ODNI). 2012. *Presidential Memorandum: National Insider Threat Policy.* November. https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf.

Trump, Donald. 2019. Executive Order 13859. *Maintaining American Leadership in Artificial Intelligence*. Federal Register, v.84, no.31 (14 February): 3967.

Trump, Donald, and The United States. 2020. *National Strategy to Secure 5G of the United States.* March. https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.