

# High Value Asset Control Overlay

Version 1.0

November 2017

Office of Cybersecurity & Communications  
*Federal Network Resilience Division*



Homeland  
Security




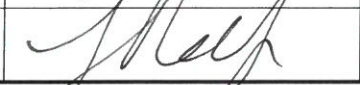
**OFFICE OF CYBERSECURITY AND COMMUNICATIONS**  
**RECORD OF COORDINATION AND APPROVAL**

<b>SUBJECT</b>	<b>PERSON TO CONTACT ON ATTACHED</b>	
20171103.13 [FOR A/S SIGNATURE] Action Memo – HVA Control Overlay	<b>NAME/OFFICE</b> Martin Stanley, Branch Chief, CAB	<b>TELEPHONE</b> 202-317-0568

**DESCRIPTION/EXPLANATION**

Seeking A/S approval for version 1.0 of HVA Control Overlay as DHS guidance for agencies to further secure HVA systems..

<b>RELEASED FOR COORDINATION</b>			
	<b>SIGNATURE</b>	<b>DATE</b>	<b>DEADLINE FOR COORDINATION</b> <b>5PM 11/10/2017</b>

OFFICE	SIGNATURE	DATE	CONCUR		NON-CONCUR	REASON
			NO COMMENT	COMMENT		
Jaffe, Judd, Kent CS&C Exec Sec		11/07/17		X		
Daniel V. Medina CS&C CoS		11/7/17	X			
Richard J. Driggers CS&C DA/S		11/9/17	X			
Jeanette Manfra CS&C A/S		11/9/17	X			

**ADDITIONAL NOTES:**  
 CS&C Exec: Task created by FNR, approved by OGC, NCCIC, NSD, and FNR in ESTT

## INTRODUCTION

Federal Government High Value Assets (HVA) enable essential functions and operations, provide services to citizens, generate and disseminate information, and facilitate greater productivity and economic prosperity.<sup>1</sup> OMB Memorandum M-16-04 “Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government,” October 30, 2015, was issued in response to the increasing number of incidents involving Federal Information Technology assets. In an effort to heighten the urgency of risk management for HVA systems, OMB issued M-17-09 “Management of Federal High Value Assets” on December 2016. The OMB memorandum provides general guidance for the planning, identification, categorization, prioritization, reporting, assessment, and remediation of HVAs.

This HVA Control Overlay (the Overlay) was developed by Office of Cyber Security and Communications (CS&C) at the Department of Homeland Security (DHS) to provide further technical guidance to federal civilian agencies to secure HVAs. The purpose of this document is to provide additional specifications for protections applied to HVAs in order to increase the level of assurance that HVAs meet the protection needs of the organizations that rely on them and the Federal Government writ large to manage and reduce known risks.

### Overlay Characteristics

The specifications in the Overlay are driven based on the criticality of the systems that it applies to and the exigence of the threats which face them. This determination is based on historical incident data, analysis of existing HVA systems, and current cyber threats known to DHS. Analysis of this information resulted in the specific selection of security controls to reduce the risks to systems and information.

NIST SP800-53r5 provides the overlay construct to extend or tailor initial control baselines through the addition or removal of controls, specifying the application of controls that are necessary for system protection, providing control extensions (i.e., additional protections) to existing controls, and specifying values for organizationally-defined parameters.

This Overlay is baseline agnostic and does not encompass all controls necessary to protect HVAs and is intended to be applied to HVAs after selecting and applying either the High or Moderate baseline as specified in NIST SP800-53r5.

### Applicability

The Overlay was created for application to Federal HVA systems as defined in OMB M-17-09.

Per OMB M-17-09 "High Value Assets" are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.<sup>2</sup>

This Overlay may also be used in full or in part to protect non-HVA systems against cyber threats after application of the appropriate baseline.

---

<sup>1</sup> OMB Memorandum M-17-09 “Management of Federal High Value Assets”

<sup>2</sup> OMB M-17-09 Management of Federal High Value Assets

The Overlay represents a starting point for ensuring HVA protections are in place. Application of the Overlay does not remove the requirement or need to apply additional overlays which may be required by regulation, statute, or threat, in a risk-based manner, to protect HVAs. In particular it may be necessary to apply multiple overlays to the selected security control baseline for the HVA (e.g., privacy overlay, industrial control system overlay, etc.). For example, HVA system with Personally Identifiable Information (PII) applies the HVA and Privacy overlays. If use of multiple overlays result in conflicts of security controls, a risk assessment should be performed to determine the appropriate actions to resolve the conflict. To realize the security objectives of the Overlay, all controls identified below should be applied as specified.

This Overlay may be revised in the future as necessary based on updates to the HVA definition, emerging threats, and the discovery of additional protections for HVAs that would further assure the protection needed at the organizational and federal level.

## High Value Asset Concerns

This initial release of the Overlay focuses on control families identified from the results of previous HVA Assessments conducted by DHS, combined with up-to-date threat information regarding government information and systems. Controls have been selected and enhanced where appropriate to reduce the following risks:

- Reduce risk of lateral movement from adjacent components through segmentation and strict flow control.
- Reduce attack surface.
- Protect against unauthorized access using strict identity and account management practices.
- Reduce and limit permissions, and strengthen access control for privileged accounts.
- Protect, control, and monitor data shared outside the HVA authorization boundary.
- Minimize data shared over interconnections to reduce the risks of loss of confidentiality outside the authorization boundary.
- Consolidate and centralize device audit and logging to facilitate monitoring to improve capabilities to detect threats.
- Ensure contractors are held accountable and liable for implementation and effectiveness of security controls.
- Protect the acquisition supply chain for devices supporting HVAs.
- Ensure HVA security is transparent and meets the needs of all stakeholders.

The Overlay specifies security control implementations in order 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 provides a defense-in-depth approach which limits and monitors access to critical components to ensure protection from the loss of confidentiality, integrity, and availability. The combination of controls in the Overlay also serves to further protect HVAs from insider threats as well as external threats. Lastly, the security controls within the Overlay consider protections necessary to secure HVAs from environments in which they operate including co-located systems, interconnected systems, enterprise services, support systems, systems protected at a lower security categorization level, and users. The Overlay primarily specifies controls applied to the HVA itself; however, there are subset of the Overlay controls that are applied at the Enterprise-level to achieve the protection objectives described above. HVAs may inherit additional overlay controls from the Enterprise that require further strengthening of those controls at the Enterprise-level in accordance with the Overlay.

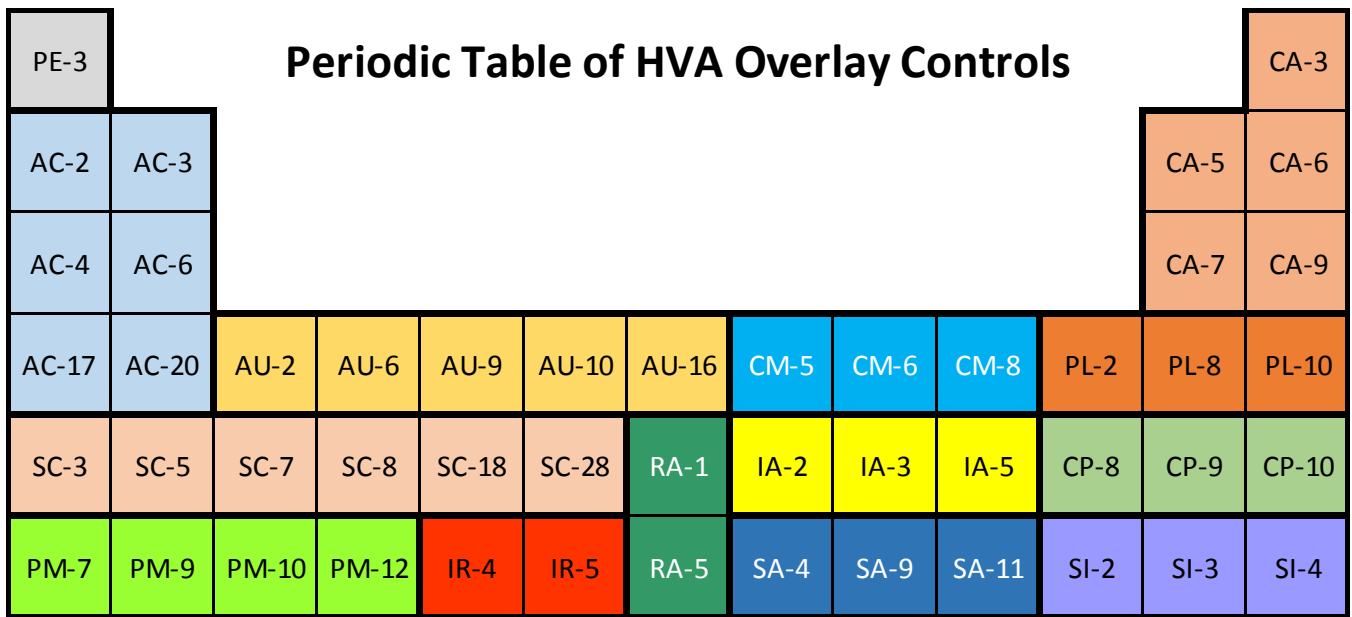
### Overlay Summary

Table 1 contains a control that is specified as not to be implemented on any HVA system and the justification as to why the control is not to be implemented. Implementation of this control introduces unacceptable risk to the HVA.

**Table 1. Prohibited Security Controls for HVAs**

CONTROL	JUSTIFICATION NOT TO SELECT
AC-2 (9)	Shared and group account actions cannot be traced back to an individual. Shared and group accounts are prohibited on HVA systems.

Figure 1 identifies the families of controls addressed in the Overlay.



AC: Access Control
AU: Audit and Accountability
CA: Assessment, Authorization, and Monitoring
CM: Configuration Management
CP: Contingency Planning
IA: Identification and Authentication
IR: Incident Response

PE: Physical and Environmental Protection
PL: Planning
PM: Program Management
RA: Risk Assessment
SA: System and Services Acquisition
SC: System and Communications Protection
SI: System and Information Integrity

**Figure 1. Periodic Table of HVA Overlay Controls**

Table 2 contains a summary of the Enterprise security controls as they apply in the Overlay. Refer to “Enterprise Controls” section of this document for more details.

**Table 2. Summary of Select Enterprise Overlay Security Controls**

<b>ID</b>	<b>FAMILY</b>	<b>CONTROL NUMBER</b>	<b>CONTROL NAME</b>
AU	Audit and Accountability	AU-6(3)	Audit Review, Analysis, and Reporting
		AU-6(4)	Audit Review, Analysis, and Reporting
		AU-6(5)	Audit Review, Analysis, and Reporting
CP	Contingency Planning	CP-8(5)	Telecommunications Services
IR	Incident Response	IR-4(4)	Incident Handling
PM	Program Management	PM-7	Enterprise Architecture
		PM-9	Risk Management Strategy
		PM-10	Security Authorization Process

## HIGH VALUE ASSET CONTROLS

This section details the security controls as they apply to the Overlay. The guidance provided in this section expands on the guidance contained in NIST SP 800-53rev5. A security control may have other specifications that include control extensions, supplemental guidance, and parameter values.

### AC-2, ACCOUNT MANAGEMENT

Control Selection Rationale	Management of user and system accounts is critical in establishing an effective access control framework for the environment and systems. The access control framework provides the mechanisms to control and limit access to individuals that have a need to access the HVA information and systems.
Parameter Value	<p>Item e Require approvals by at least two appropriate organizational personnel (System owner, mission/business owner, AO, Chief Information Security Officer, etc.) for requests to create system accounts.</p> <p>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.</p> <p>Item j Review privileged accounts, at least, quarterly for compliance with account management requirements. Privileged account access to be reauthorized for the HVA at least annually. Review user accounts, at least, annually for compliance with account management requirements.</p>
Related Controls	AC-3, AC-6, AC-17, AC-20, AU-9, IA-2, IA-8, SC-7.
References	OMB Circular A-130

### AC-2, Control Enhancement 2, ACCOUNT MANAGEMENT / REMOVAL OF TEMPORARY AND EMERGENCY ACCOUNTS

Control Selection Rationale	Temporary and Emergency accounts are considered high-risk accounts and are tightly controlled, monitored, and removed promptly when no longer required to avoid unauthorized access to the HVA.
Parameter Value	Automatically disable temporary and emergency accounts within 12 hours of issuance. This reduces the risk that Temporary and Emergency accounts, which typically do not have multi-factor authentication, are not a source of compromise.

### AC-2, Control Enhancement 14, ACCOUNT MANAGEMENT / PROHIBIT SPECIFIC ACCOUNT TYPES

Control Selection Rationale	Guest, anonymous and shared account actions cannot be traced back to an individual which could result in unauthorized access and exfiltration of HVA information.
Parameter Value	Prohibit the creation and use of guest, anonymous, and shared accounts (including shared administrator and root accounts) for access to all information types processed by the system. NOTE: Anonymous is allowed for public information websites only.
References	OMB Circular A-130



**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.
Supplemental Guidance	Organizations control access to systems and 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).
Related Controls	AC-2, AC-4, AC-6, AC-17, AC-20, AU-9, CA-9, IA-2, IA-5, SC-2, SC-3, SI-4
References	OMB Circular A-130

**AC-3, Control Enhancement 9, ACCESS ENFORCEMENT / CONTROLLED RELEASE**

Control Selection Rationale	Systems 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 system boundaries. HVA information shared or exchanged outside the authorization boundary may be at increased risk of unauthorized access and use.				
Control Extension	Organization procedures for sharing or releasing information outside the HVA authorization boundary protect the information through agreements. Organizations limit the sharing of information to only the attributes required by the receiving entity. A risk assessment performed on the reduced dataset determines the level of risk and level of protection required to protect the information. Organizations consider validating effective implementation of security protections through technical reviews or inspections of the external entities systems.				
Parameter Value	<table border="0"> <tr> <td style="vertical-align: top;">Item a</td> <td>The external system provides a level of protection commensurate with the confidentiality, integrity, and availability impact levels of the information being shared.</td> </tr> <tr> <td style="vertical-align: top;">Item b</td> <td>The external entity provides a copy of the Authorization to Operate (ATO) for the system that will process, store, or transmit the HVA information. The ATO is current and signed.</td> </tr> </table>	Item a	The external system provides a level of protection commensurate with the confidentiality, integrity, and availability impact levels of the information being shared.	Item b	The external entity provides a copy of the Authorization to Operate (ATO) for the system that will process, store, or transmit the HVA information. The ATO is current and signed.
Item a	The external system provides a level of protection commensurate with the confidentiality, integrity, and availability impact levels of the information being shared.				
Item b	The external entity provides a copy of the Authorization to Operate (ATO) for the system that will process, store, or transmit the HVA information. The ATO is current and signed.				
References	OMB Circular A-130				

**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.
Parameter Value	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.
Related Controls	AC-3, AC-6, AC-17, AU-10, CA-9, SC-7
References	OMB Circular A-130

**AC-6, LEAST PRIVILEGE**

Control Selection Rationale	Control and limit access for HVA users in accordance with the principle of least privilege. Granting only the necessary rights to support the mission and business function ensures the protection of the information and mission critical services at a level commensurate with the risk to the system and information.
Supplemental Guidance	Organizations control access (user and resource accounts) to information, not identified as public information, through identification and authentication solutions that limits access to only the necessary rights and permissions required for the user. The Overlay specifies that regular user accounts not have local administration rights on any systems. Privileged accounts are required to perform privileged actions.
Related Controls	AC-2, AC-3, PL-2
References	OMB Circular A-130

**AC-6, Control Enhancement 5, LEAST PRIVILEGE / PRIVILEGED ACCOUNTS**

Control Selection Rationale	Privileged accounts are targeted by adversaries because of the elevated rights granted to those accounts. To protect against unauthorized access or loss of integrity privileged accounts are protected at a higher level than non-privileged accounts.
Control Extension	Privileged accounts are not allowed access to other networks or systems outside the authorization boundary (i.e. the Internet, other internal systems).
Parameter Value	Privileged accounts have restricted and limited rights to functions, services, and attributes necessary to perform the required tasks.
Related Controls	IA-2, AC-4, CM-6
References	OMB Circular A-130

**AC-6, Control Enhancement 7, LEAST PRIVILEGE / REVIEW OF USER PRIVILEGES**

Control Selection Rationale	Account reviews are performed on a periodic basis to ensure that user access permissions are still relevant and necessary to ensure that they cannot be leveraged for unauthorized access. Given the sensitivity of the HVA system and information the frequency of the account reviews are increased.
Parameter Value    Item a	At a minimum, review annually the rights assigned to user accounts and validate the need for such rights. At a minimum, review quarterly the rights assigned to privileged accounts and validate the need for such privileges.
Related Controls	CA-7
References	OMB Circular A-130

**AC-17, REMOTE ACCESS**

Control Selection Rationale	Controlling and limiting access to the HVA environment from remote locations (outside the HVA authorization boundary) ensures the protection of the HVA information and integrity of the controls implemented and operating in the environment.
-----------------------------	---

Supplemental Guidance	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-20, IA-2, IA-3, IA-8, PL-2, SI-4
References	OMB Circular A-130, NIST SP800-46, NIST SP800-77, NIST SP800-113

**AC-17, Control Enhancement 2, REMOTE ACCESS / PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION**

Control Selection Rationale	Protecting the confidentiality and integrity of remote access data/sessions ensure HVA information is protected from unauthorized access in transit.
Supplemental Guidance	To protect information during transmission FIPS 140-2 compliance encryption is specified for all remote access sessions over networks outside the HVA authorization boundary.
Related Controls	SC-8
References	OMB Circular A-130

**AC-20, USE OF EXTERNAL SYSTEMS**

Control Selection Rationale	Protecting the HVA information from loss of confidentiality or integrity when accessing or processing HVA information on external systems or environments requires strict terms and conditions consistent with security and privacy requirements for federal systems protected at a level congruent with the HVA information.
Control Extension	Organizations establish detailed terms and conditions of acceptable use, in accordance with organizational security policies and procedures and federal guidelines and laws. At a minimum these terms and conditions (contractual requirements for vendors/consultants) shall 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.
Related Controls	AC-2, AC-3, AC-17, CA-3, PL-2, SA-9, SC-7
References	OMB Circular A-130, FIPS 199

**AU-2, AUDIT EVENTS**

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.
Supplemental Guidance	The parameter value (item d) 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.
Parameter Value    Item d	Audit success and failed logons (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 IP, port and protocol; Destination IP, port and protocol; Etc.
Related Controls	AC-2, AC-3, AC-6, AC-17, CM-6, IA-3, PE-3, SC-7, SC-18, SI-3, SI-4, SI-10, SI-11
References	OMB Circular A-130, US-CERT “Federal Incident Reporting Guidelines”, NIST SP800-92

**AU-6, AUDIT 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.
Supplemental Guidance	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.
Parameter Value	Item a Review, analyze, and alert on system audit records in real-time for indications of inappropriate, unusual activity (i.e, concurrent logons), breaches, or threats.
	Item b Report incidents and findings in accordance with US-CERT reporting timeframes and requirements.
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 SP800-92

**AU-9, PROTECTION OF AUDIT INFORMATION**

Control Selection Rationale	Audit information is protected at the same level as the system that generated the audit information. To ensure that any potential HVA information contained within audit logs is protected adequately.
Supplemental Guidance	The storage of audit information is protected to the highest level commensurate with the security protection level of the highest information contained within the audit events.
Related Controls	AC-3, AC-6, AU-6, PE-3, SC-8, SI-4
References	OMB Circular A-130, NIST SP800-92

**AU-9, Control Enhancement 2, PROTECTION OF AUDIT INFORMATION / STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS**

Control Selection Rationale	Protection of audit information integrity on the systems is critical for accurate and timely incident response management and accountability.
Supplemental Guidance	Organizations protect system audit information by storing/transferring audit information to a physically different system from the system that generated the events.
References	OMB Circular A-130, NIST SP800-92

**AU-9, Control Enhancement 3, PROTECTION OF AUDIT INFORMATION / CRYPTOGRAPHIC PROTECTION**

Control Selection Rationale	Protection of audit information integrity on the system is necessary for accurate accountability and traceability of actions on the HVA.
-----------------------------	--

Supplemental Guidance	Implement cryptographic solutions (i.e. hashing function) to protect the integrity of audit information at rest.
Related Controls	AU-10
References	OMB Circular A-130

**AU-9, Control Enhancement 5, PROTECTION OF AUDIT INFORMATION / DUAL AUTHORIZATION**

Control Selection Rationale	Protection of audit log management is critical in ensuring that the integrity of logs is maintained and assured for accountability of user actions.
Supplemental Guidance	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 organizational personnel (System owner, mission/business owner, AO, Chief Information Security Officer, 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.
Parameter Value	Enforce dual authorization (two appropriate organizational personnel such as system owner, mission/business owner, AO, Chief Information Security Officer, etc.) for manual movement and deletion of system audit logs.
Related Controls	AC-3
References	OMB Circular A-130

**AU-9, Control Enhancement 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.
Supplemental Guidance	Only limited privilege accounts with the need to know have read-only access to audit logs. All others 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.
Parameter Value	Access to audit logs are read-only for authorized individuals (Privileged accounts only).
Related Controls	AU-9(5)
References	OMB Circular A-130

**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.
Supplemental Guidance	The HVA provides for 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
Related Controls	AU-9, SC-8
References	OMB Circular A-130

**AU-16, CROSS-ORGANIZATIONAL AUDITING**

Control Selection Rationale	Organizations using external systems and services to support the HVA maintain auditing capabilities, non-repudiation of the users, and correlation of actions across the external systems to allow for accurate and timely incident response capabilities.
Parameter Value	Organizations require that the contractor or external hosting entity comply with federal and agency audit requirements in the external environments. The external system provides non-repudiation for non-public user access to HVA information for accountability.
Related Controls	AU-6
References	OMB Circular A-130; NIST SP800-150

**CA-3, SYSTEM INTERCONNECTIONS**

Control Selection Rationale	Organizations 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.
Supplemental Guidance	<p>Organizations create, authorize, and track ISA documents for each external support services and each external connection (outside the authorization boundary) to and from the HVA.</p> <p>In the case of external connections, the ISA includes technical details to include but not limited to: IP addresses, 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.</p> <p>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.</p> <p>The organization develops and implements a Memorandum of Understanding/Agreement (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.</p> <p>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.</p>
Parameter Value	ISA and MOU/A shall be reviewed and updated at least annually and in response to environmental or operational changes to either system.
Related Controls	AC-20, AU-16, IA-3, SA-9, SC-7
References	OMB Circular A-130, FIPS 199, NIST SP800-47

### CA-3, Control Enhancement 5, SYSTEM INTERCONNECTIONS / RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

Control Selection Rationale	Connecting HVAs or exchanging information with external systems increases the risk of a loss of confidentiality, integrity, or availability of the HVA.
Parameter Value	Deny by default, permit by exception policy for HVA Access Control to connect (all connections) or exchange information with external systems. Permitted exceptions are applied using a risk-based approach in the most restrictive as possible manner that still allows for operations (i.e. Source and destination IP address, ports, protocol, etc.).
Related Controls	SC-7, CM-7
References	OMB Circular A-130, NIST SP800-47

### CA-5, PLAN OF ACTION AND MILESTONES

Control Selection Rationale	Tracking and monitoring planned remedial actions of system weaknesses and deficiencies is specified to ensure actions are occurring for protecting the HVA information and systems. Likewise, tracking and monitoring planned remedial actions of supporting systems from which the HVA inherits controls is necessary to ensure that the HVA is not unknowingly accepting risk from these interdependencies.
Supplemental Guidance	HVA systems are to be prioritized for timely remediation of weaknesses and deficiencies to minimize the risks to the HVA. Organizations prioritize remediation efforts based on the risk to the systems; remediating highest risks first. Prioritized POA&M management informs the program, planning, budget 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.
Parameter Value	HVA systems and supporting system's Plan of Action and Milestones (POA&M) are reviewed, updated at least monthly, and signed off by the AOs (dual AOs - see AU-9 (5)) at least quarterly.
Related Controls	CA-7, SI-2
References	OMB Circular A-130, NIST SP800-47

### CA-6, AUTHORIZATION

Control Selection Rationale	Authorizations are the official Authorization to Operate (ATO) HVA systems and are issued by the Authorizing Official (AO) where the formal acceptance of the risk to organizational operations and assets, people, interconnections, and the Nation is recorded.
Supplemental Guidance	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 remediates 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-7
References	OMB Circular A-130, NIST SP800-37, NIST SP800-137



**CA-6, Control Enhancement 1, AUTHORIZATION / JOINT AUTHORIZATION – SAME ORGANIZATION**

Control Selection Rationale	Organizations that operate HVAs ensure that risks to HVAs are known to impacted parties and effectively managed and remediated. Assigning multiple AOs from the same organization to serve as co-AOs for the system 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.
Supplemental Guidance	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 SP800-37, NIST SP800-137

**CA-7, CONTINUOUS MONITORING**

Control Selection Rationale	Risks to systems are dynamic and change in real time requiring a continuous monitoring strategy be applied to HVAs to promote timely risk awareness and remediation.
Supplemental Guidance	<p>Continuous Monitoring provides continuous assurance that security controls are effectively meeting organizational protection needs. Organizations develop continuous monitoring strategy in accordance with NIST SP800-137 “Information Security Continuous Monitoring (ISCM)” to include all selected security controls in use for the systems.</p> <p>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.</p> <p>Continuous Monitoring programs follow federal guidance and reporting requirements per OMB Circular A-130 “<i>Managing Information as a Strategic Resource</i>” and comply with CDM reporting requirements. External service providers hosting HVA information and mission critical services are required to meet Federal, DHS CDM, and organizational ISCM requirements.</p> <p>Leverage ISCM capabilities to support the migration to Ongoing Authorization (OA) process.</p>
Related Controls	AC-2, AC-6, CA-5, CA-6, CM-6, IA-5, PL-2, RA-5, SA-11, SC-5, SI-3, SI-4, PE-3, SC-8, SI-4
References	OMB Circular A-130, NIST SP800-37, NIST SP800-137



**CA-7, Control Enhancement 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 against 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.
Supplemental Guidance	Organizations examine, correlate, and analyze current threat information sources, emerging vulnerabilities and exploits, latest social engineering tactics, intrusion detection events, and auditor reports and adjust the frequency and types of continuous monitoring activities, accordingly, to be performed against the systems and environment.
References	OMB Circular A-130, NIST SP800-37, NIST SP800-137, US-CERT Technical Cyber Security Alerts

**CA-9, INTERNAL SYSTEM CONNECTIONS**

Control Selection Rationale	All connections to and from the HVA environment, both internal and external, pose an increased level of risk to the HVA system and information due to potential compromise of the connected system. These connected systems may be protected at different levels than the HVA system.
Supplemental Guidance	Organizations identify the connections between HVAs and other systems, including other HVAs and non-HVAs, to understand critical dependencies <sup>3</sup> 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.
Parameter Value    Item a	Internal connections between the HVA environment and other organizational systems (including support systems) are documented and authorized. Organizations may choose to develop a streamlined version of a typical Interconnection Security Agreements (ISA)/Memorandum of Understanding (MOU) to be used for internal connections.
Related Controls	AC-3, AC-4, IA-3, SC-7
References	OMB Circular A-130

**CM-5, Control Enhancement 2, ACCESS RESTRICTIONS FOR CHANGE / REVIEW SYSTEM CHANGES**

Control Selection Rationale	Reviewing and monitoring systems for unauthorized changes identifies potential malicious activities that can lead to compromise of information, loss of integrity, or loss of availability.
Parameter Value	Review system for changes no less than monthly, and upon unscheduled or unplanned system restarts to determine whether unauthorized changes have occurred. This review can be automated to simplify the task and increase the frequency of the review.
Related Controls	AU-6
References	OMB Circular A-130

**CM-6, CONFIGURATION SETTINGS**

Control Selection Rationale	Developing and tracking baseline configurations of HVAs allows for establishment of common configurations for the systems to allow for better
-----------------------------	---

<sup>3</sup> OMB M-17-09 requirements

	detection of unauthorized modification or changes which could indicated a compromise of information and mission critical services.
Supplemental Guidance	Establish and document baseline configuration settings for HVA components and track deviations from these established baseline for all systems and devices that comprise the HVA. Configuration settings apply to HVA systems and components and changes to configuration settings are monitored, tracked, and controlled.
Control Extension	Ensure baseline configurations enforce secure authentication: Admin Password reuse issue: Do not allow for a common local administrator password on all the workstations, servers, and systems; Insecure default configuration: Ensure that default configurations of COTS products are modified and not left as default. Verify the default configurations are not reverted to each time the COTS packages are updated or upgraded; Default application password(s): Change all default passwords on COTS/GOTS and device products.
Related Controls	AC-3, AU-2, AU-6, CA-9, IA-3, IA-5, PL-8, RA-5, SA-4, SA-9, SC-18, SC-28, SI-2, SI-4
References	OMB Circular A-130

**CM-6, Control Enhancement 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.
Supplemental Guidance	Organizations cross reference detected changes with change control documentation to determine if the change was preauthorized. Organizations are prepared for action and processes documented on detection of unauthorized changes to systems. Organizations 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.
References	OMB Circular A-130

**CM-8, INFORMATION 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.
Supplemental Guidance	Organizations implement automated solutions to perform component inventory of the environment within the DHS CDM requirement timeframe.
Parameter Value    Item b	Review and update the system device inventory at least every 72 hours consistent with DHS CDM reporting requirements.
Related Controls	SI-2
References	OMB Circular A-130, DHS CDM Reporting Requirements

**CP-9, Control Enhancement 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.
Supplemental Guidance	As part of the contingency planning processes organizations restore complete select system functions to ensure that backups are effective, organization

	personnel know how to perform function restores, and technically the function operates correctly once restored.
References	OMB Circular A-130, NIST SP800-34

**CP-10, Control Enhancement 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.
Supplemental Guidance	Organizations determine, develop, and implement the capability to restore the system within a defined restoration time in accordance with organizational system availability impact risk assessment.
References	OMB Circular A-130, NIST SP800-34

**IA-2, IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**

Control Selection Rationale	To ensure accountability of actions the HVA uniquely identifies all users, systems, and services acting on behalf of organizational users.
Supplemental Guidance	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 must not utilize well known account IDs (e.g. 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-17, AU-6, IA-5, IA-8, SA-4
References	OMB Circular A-130, OMB M-16-04, OMB M-11-11, FIPS 201, NIST SP800-63

**IA-2, Control Enhancement 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.
Supplemental Guidance	Organizations ensure that privileged accounts are authenticated on each system using multifactor authentication mechanisms to protect against password weaknesses. All systems and devices support and implement authentication of privileged accounts through multifactor authentication.
References	OMB Circular A-130, OMB M-16-04, OMB M-11-11, FIPS 201, NIST SP800-63

**IA-2, Control Enhancement 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.
Supplemental Guidance	Organizations ensure that non-privileged accounts are authenticated on each system using multifactor authentication mechanisms to protect against password

	weaknesses. All systems and devices support and implement authentication of non-privileged accounts through multifactor authentication.
References	OMB Circular A-130, OMB M-16-04, OMB M-11-11, FIPS 201, NIST SP800-63

**IA-2, Control Enhancement 12, IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / ACCEPTANCE OF PIV CREDENTIALS**

Control Selection Rationale	HSPD-12 requires federal agencies to implement Personal Identity Verification (PIV) credentials for identification and authentication.
Supplemental Guidance	Identification and authentication to HVA shall be facilitated using PIV in compliance with FIPS Publication 201-1 and OMB M-11-11. Additional authentication factors shall be employed in a risk-based manner.
References	OMB Circular A-130, OMB M-16-04, OMB M-11-11, FIPS 201, NIST SP800-63

**IA-3, DEVICE IDENTIFICATION AND AUTHENTICATION**

Control Selection Rationale	Device authentication protects against unauthorized devices from accessing HVA information and services.
Supplemental Guidance	Organizations ensure that only authorized devices can connect to the HVA environment.
Parameter Value	Validates security posture, uniquely identifies, and authenticates devices before establishing a network connection to the HVA.
Related Controls	AC-17, AU-6, CA-3, CA-9, IA-5, SI-4
References	OMB Circular A-130

**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.
Parameter Value	Item f Changing/refreshing authenticators at least annually for cryptographic devices.
	Item f Changing/refreshing authenticators at least annually or upon departure of key personnel with knowledge of password for service and system account passwords/pins.
Related Controls	AC-3, AC-6, CM-6, IA-2, IA-8
References	OMB Circular A-130, OMB M-16-04, OMB M-11-11, FIPS 201, NIST SP800-63

**IA-5, Control Enhancement 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.
Supplemental Guidance	User and privileged accounts must comply with multifactor authentication requirements. Service and System accounts that leverage password based authentication shall meet the following requirements: Passphrases consisting solely of letters 20 or more characters in length; Default authentication credentials are not used; Passwords must be changed at least annually, or upon personnel turnover; Passwords shall be stored in a secured location and only used when

	necessary; Passwords shall be unique for each identifier and on each system within the HVA boundary; and Password reuse is not permitted.
References	OMB Circular A-130, OMB M-16-04, OMB M-11-11, FIPS 201, NIST SP800-63, NIST SP800-132

**IR-4, Control Enhancement 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.
Supplemental Guidance	Incident response plans for HVA incorporate external interconnected entities to ensure collaboration and reporting of appropriate information. ISA/MOU/MOAs shall include incident response requirements and reporting timeframes for all entities that interoperate with the HVA in accordance with US-CERT incident handling and Federal Reporting requirements.
Related Controls	AU-16
References	OMB Circular A-130, NIST SP800-61 R2

**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 Extension	Organizations monitor, track, and report incidents accurately in accordance with US-CERT “Federal Incident Notification Guidelines” <sup>4</sup> . Organizations monitor all interconnected traffic into and out of the HVA to detect threats, and abnormal or malicious communications. Organizations 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.
Related Controls	AU-6, SC-5, SC-7, SI-3, SI-4
References	OMB Circular A-130, NIST SP800-61 R2

**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 Extension	Physical Access Authorizations to HVA systems and environment is authorized using dual authorizations. Physical access to environments housing HVA components require two authorized individuals within the organization to approve a requestor’s physical access to HVA. Physical Access requests are reauthorized at least annually.
Related Controls	AU-2, AU-6, AU-9, IA-3, IA-8, PE-5, SC-28, SI-4
References	OMB Circular A-130, FIPS 201

**PE-3, Control Enhancement 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.
-----------------------------	--

<sup>4</sup> <https://www.us-cert.gov/government-users/reporting-requirements>

Supplemental Guidance	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.
References	OMB Circular A-130, FIPS 201

**PL-2, SECURITY AND PRIVACY PLANS**

Control Selection Rationale	HVA Security and Privacy Plans provide specific details regarding the implementation of the system and the rationale for the selection of security controls to protect the HVA from threats.
Supplemental Guidance	<p>HVA Security and Privacy Plans are complete and include sufficient detail regarding the security approach to protecting the HVA. Descriptions of tailored controls include a detailed justification as to why the control was included or not. Each control description details how it has been implemented. Controls descriptions inherited from another system provide sufficient detail regarding how the control implementation meets the control requirement for the HVA.</p> <p>HVA Security and Privacy plans minimally include 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 (HVA, Privacy, etc.); Control tailoring details and supporting rationale; and Detailed description of the implementation of each security control.</p> <p>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.</p>
Related Controls	AC-2, AC-6, AC-17, AC-20, CA-3, CA-7, CA-9, PL-8
References	OMB Circular A-130, NIST SP800-18

**PL-8, SECURITY AND PRIVACY ARCHITECTURES**

Control Selection Rationale	The architecture of the HVA environment must protect the information and supported missions from loss of confidentiality, integrity or availability. The architecture must 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).
Supplemental Guidance	<p>In accordance OMB M-17-09 organizations: Ensure strict access control implementation; Multifactor authentication; Vulnerability scanning; Increased monitoring and analysis of events; Network segmentation; Boundary protections; and Incident response testing</p> <p>The HVA security architecture is 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.</p> <p>Detailed data flows of information within the HVA are developed and prioritized, rules and policies are created where segmentation, and layers of isolation are identified.</p>



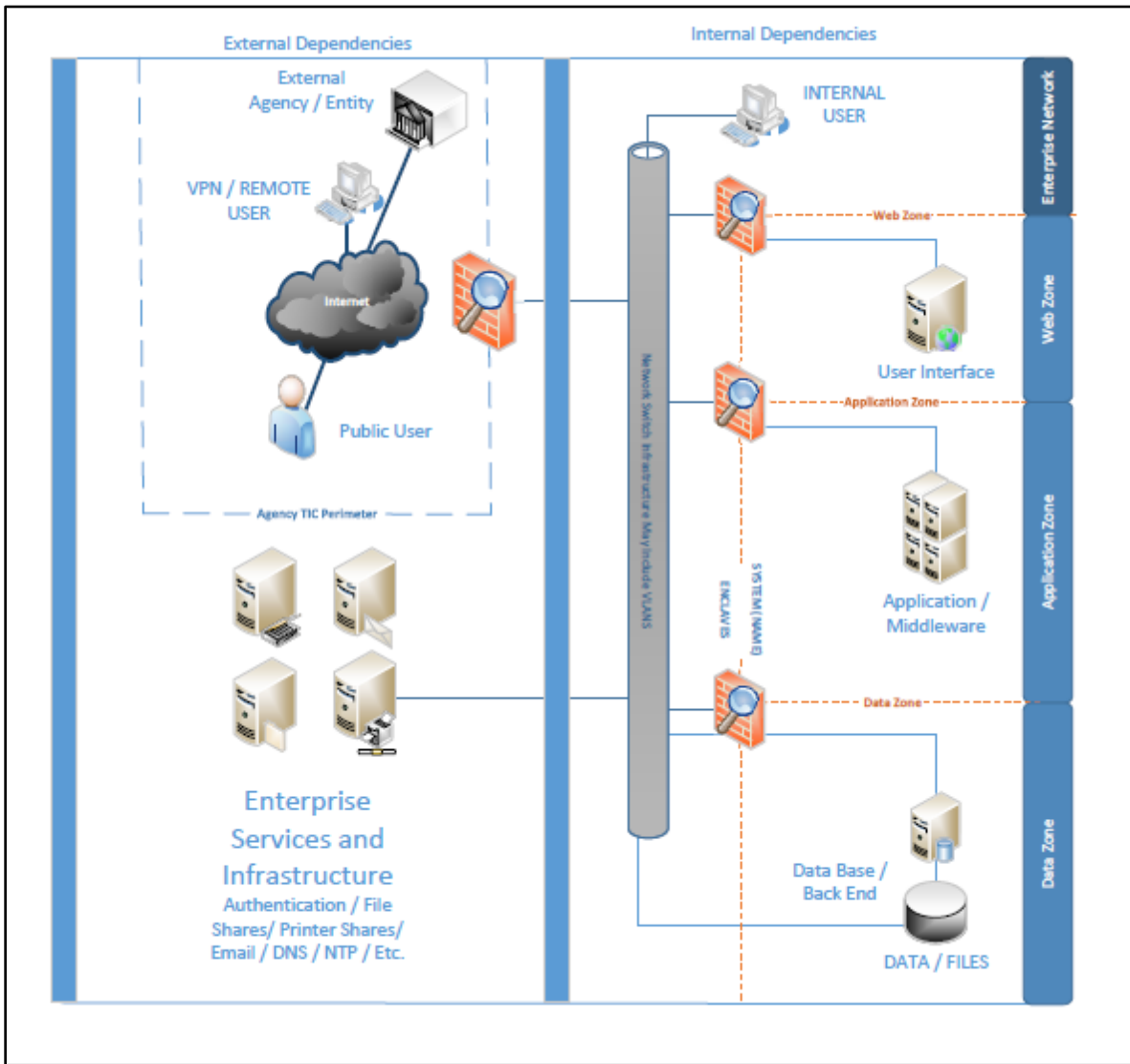
	Devices that do not require direct access by HVA users are located behind boundary protection devices with strict access control, filtering, and monitoring. Access lists are default deny, permit by exception both inbound and outbound. Egress rules block all access except required services. Block all unnecessary traffic to the Internet. Security and Administrative services and functions are isolated onto their own networks with strict access control. Implement access control lists to limit traffic between security, admin, and production networks. Traffic entering and leaving the HVA accreditation boundary is encrypted in accordance with the risk analysis of the information being transmitted. Device services and applications are only bound to the appropriate interface/network required for it to function.
Related Controls	CM-6, PL-2
References	OMB Circular A-130, NIST SP800-160

**PL-8, Control Enhancement 1, SECURITY AND PRIVACY ARCHITECTURES / DEFENSE-IN-DEPTH**

Control Selection Rationale	Protecting sensitive information behind multiple layers of security boundaries ensures that adversaries must circumvent multiple security mechanisms to compromise HVA information and services.
Supplemental Guidance	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.
References	OMB Circular A-130, NIST SP800-160

*Figure 2. Sample Architecture*





**PL-10, BASELINE SELECTION**

Control Selection Rationale	Security categorization of HVA is performed in accordance with Federal Information Processing Standards (FIPS) 199. Additional controls for HVA systems are applied in a risk-based manner in accordance with the Federal Information Security Modernization Act (FISMA) and the Privacy Act to ensure that sufficient security measures are implemented to protect HVAs.
Control Extension	At a minimum all HVA systems start with at least the Moderate baseline from NIST SP 800-53 R5. All HVA overlay controls must be applied as specified and are not tailored.
Supplemental Guidance	Organizations leverage FIPS 199 system categorization to select and tailor the initial baseline controls for HVA from NIST SP800-53 R5 (Moderate or High baselines only). All HVA systems also receive the controls in the HVA overlay. Based on a risk assessment and the types of information stored/transmitted/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	RA-2
References	OMB Circular A-130, FIPS 199

## RA-2, SECURITY CATEGORIZATION

Control Selection Rationale	To provide the necessary level of assurance to stakeholders, organizations 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 Extension	Based on the definition of the impacts defined in FIPS 199 all HVAs shall be categorized no lower than Moderate.
Supplemental Guidance	Organizations apply the “high water mark” concept to their HVA systems categorized in accordance with FIPS 199 (at no less than the moderate level).
Related Controls	CM-8, PL-2, PL-10, RA-5, SC-7
References	OMB Circular A-130, FIPS 199, NIST SP800-30, NIST SP800-60

## RA-5, VULNERABILITY SCANNING

Control Selection Rationale	Timely identification of vulnerabilities in the HVA is critical in ensuring that HVA systems and components are protected from compromise due to vulnerabilities of the systems.
Supplemental Guidance	Organizations consider performing credentialed agent based or credentialed workstation based vulnerability scans to comply with 72 hour requirement
Parameter Value    Item a	Organizations implement vulnerability scanning capabilities to discovery and identify known flaws on the components at least every 72 hours <sup>5</sup> .
Related Controls	CM-6, CM-8, RA-2, SA-11, SA-12, SI-2, SI-3, SI-4
References	OMB Circular A-130, DHS CDM program

## SA-4, ACQUISITION PROCESS

Control Selection Rationale	Contracts for HVA system support, services, and solutions comply with security requirements of the Federal government and relevant organizational policies and procedures to ensure that the contractors are protecting the information and systems at the appropriate levels.
Control Extension	Contract agreements for support or services of HVA systems and environment must include requirements for the application of the HVA control overlay. Contractor agreements incorporate Federal Incident Reporting Guidelines, as identified by USCERT, into Service Level Agreements.
Supplemental Guidance	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 comply with all security requirements as defined in the contractual agreements. The organization oversees and monitors the contractor’s compliance with the contract.
Related Controls	CM-6, CM-8, SA-11, SA-12
References	OMB Circular A-130, NIST SP800-37, NIST SP800-137

## SA-9, EXTERNAL SYSTEM SERVICES

Control Selection Rationale	Ensuring that 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.
-----------------------------	--

<sup>5</sup> DHS Continuous Diagnostics and Mitigation program requirement

Parameter Value	Item a	Require that providers of external services comply with organizational security and privacy requirements and comply with the specifications defined in the HVA control overlay.
Related Controls		CA-3, PL-10, SA-2, SA-4
References		OMB Circular A-130

**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 Extension	Organizations include contractual language requiring 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.
Related Controls	CA-7, SA-4, SA-12, SI-2
References	OMB Circular A-130

**SA-11, Control Enhancement 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.
Supplemental Guidance	As part of the development lifecycle, organizations ensure that static code analysis is performed on applications to identify code weaknesses and outdated or vulnerable libraries. Contractual language for contractor development requires the contractor to perform this task as part of the deliverables. Organizations also require static code analysis for all modifications, updates, or additions to applications or systems prior to implementation.
References	OMB Circular A-130

**SA-11, Control Enhancement 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 that the solution being developed is incorporating the required security capabilities and that they are operating as intended.
Supplemental Guidance	Organizations 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 incorporate threat modeling and vulnerability analysis requirements in contractual language for new and updates/upgrades/changes to existing applications. Organizations monitor and track contractor compliance with contractual requirements.
References	OMB Circular A-130

**SA-11, Control Enhancement 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.
Supplemental Guidance	Organizations 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 monitor and track contractor compliance with organizational policies and contractual requirements for manual code review.
References	OMB Circular A-130

**SA-11, Control Enhancement 5, DEVELOPER TESTING AND EVALUATION / PENETRATION TESTING**

Control Selection Rationale	Testing a new or modified application or components prior to implementation protects against possible loss of confidentiality, integrity, and availability.
Supplemental Guidance	Organizations 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 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 tests is often performed in conjunction with automated and manual code reviews to provide greater levels of analysis. Organizations monitor and track contractor compliance with contractual requirements.
References	OMB Circular A-130

**SA-11, Control Enhancement 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.
Supplemental Guidance	Organizations 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 monitor and track contractor compliance with organizational policies and contractual requirements.
References	OMB Circular A-130

**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.
Supplemental Guidance	To provide additional protection to security communications, organizations isolate security communications from production functions on networks. Organizations

	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.
Related Controls	AC-3, AC-6, AC-20, SA-4, SC-2, SC-7, SC-32
References	OMB Circular A-130

**SC-3, Control Enhancement 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.
Supplemental Guidance	Organizations implement access and flow control to and from the security functions network and other network(s) supporting the HVA environment. Organizations 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.
References	OMB Circular A-130

**SC-5, DENIAL OF SERVICE PROTECTION**

Control Selection Rationale	To ensure availability of the service the environment protects external facing systems against denial of service attacks.
Supplemental Guidance	Organizations 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.
Related Controls	SC-7
References	OMB Circular A-130

**SC-5, Control Enhancement 1, DENIAL OF SERVICE PROTECTION / RESTRICT INTERNAL USERS**

Control Selection Rationale	Denial of Service (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.
Supplemental Guidance	Boundary protection devices, both at the authorization perimeter and inside the boundary, incorporate DoS protections for all users.
References	OMB Circular A-130

**SC-5, Control Enhancement 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.
Supplemental Guidance	Organizations limit and control capacity into and out of the authorization boundary and at key points inside the boundary to ensure that sufficient capacity exists to prevent network flooding DoS. Organizations perform a risk assessment to determine the appropriate locations inside the authorization boundary based on data flow and user access.
References	OMB Circular A-130

**SC-5, Control Enhancement 3, DENIAL OF SERVICE PROTECTION / DETECTION AND MONITORING**

Control Selection Rationale	Monitoring boundary protection devices for indicators of denial of service attacks allows the organization to respond to denial of service attacks in a timely manner and thereby reducing or avoiding a loss of availability.
Supplemental Guidance	Organizations employ inspection tools to detect DoS anomalies both at the perimeter of the authorization boundary as well inside the authorization boundary on access control points that form isolation zones. The organization determines the level of inspection required for each isolation zone based on risk assessment to the HVA.
References	OMB Circular A-130

**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.
Supplemental Guidance	<p>Organization employs 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 that are protected at a lower level of trust must be implemented in a manner that reduces the risk that these interdependencies may introduce to the HVA.</p> <p>Examples of boundary protection devices include: Firewalls; Application Firewall/Proxy/Gateway (web, email, data transfers, etc.); Intrusion Detection; Service/Intrusion Prevention Service; and Application Load Balancer/ Cryptographic services.</p> <p>Organizations implement default deny; permit by exception for egress and ingress access control at the boundary. All devices are 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 shall not be used in allow access control statements. Systems and components within the HVA environment do not have direct access to the internet unless specifically required for the application to function. It is recommended to block HTTP &amp; HTTPS traffic bi-directionally for all internal systems.</p>
Related Controls	AC-4, AC-17, AC-20, CA-3, PE-3, SC-5, SC-32



References	OMB Circular A-130
------------	--------------------

**SC-7, Control Enhancement 10, BOUNDARY PROTECTION / PREVENT UNAUTHORIZED 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 Extension	Organizations implement technical measures and enhanced inspection of traffic flow into and out and within the authorization boundary. Enforcing protocol validation checking, traffic monitoring, packet inspection, SSL packet inspection, beaconing traffic, to name a few to be implemented on the authorization boundary devices and isolation devices throughout the environment.
Related Controls	AC-3
References	OMB Circular A-130

**SC-7, Control Enhancement 11, BOUNDARY PROTECTION / RESTRICT INCOMING COMMUNICATIONS TRAFFIC**

Control Selection Rationale	Restricting access through the authorization boundary to only authorized traffic limits the exposure to threats and reduces the attack surface of the HVA.
Control Extension	Organizations implement incoming communications control for the HVA at the authorization boundary. Access control is restrictive and specific as possible. The use of wildcards in ALLOW rules (ANY or ALL) shall not be used. Default deny ANY rules with logging are enabled.
Related Controls	AC-3
References	OMB Circular A-130

**SC-7, Control Enhancement 12, BOUNDARY PROTECTION / HOST-BASED PROTECTION**

Control Selection Rationale	Protecting HVA from compromise due to lateral attack from adjacent systems or from direct attacks ensures the confidentiality, integrity, and availability of the information and systems.
Supplemental Guidance	As part of a defense in depth approach, implement host-based protections (e.g. firewall, HIDS, HIPS) on the HVA system components to protect the HVA from unauthorized access or compromise. Organizations monitor these system activities as part of the incident monitoring processes and procedures.
References	OMB Circular A-130

**SC-7, Control Enhancement 14, BOUNDARY PROTECTION / PROTECTS 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.
Supplemental Guidance	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) that contains the HVA components.



References	OMB Circular A-130
------------	--------------------

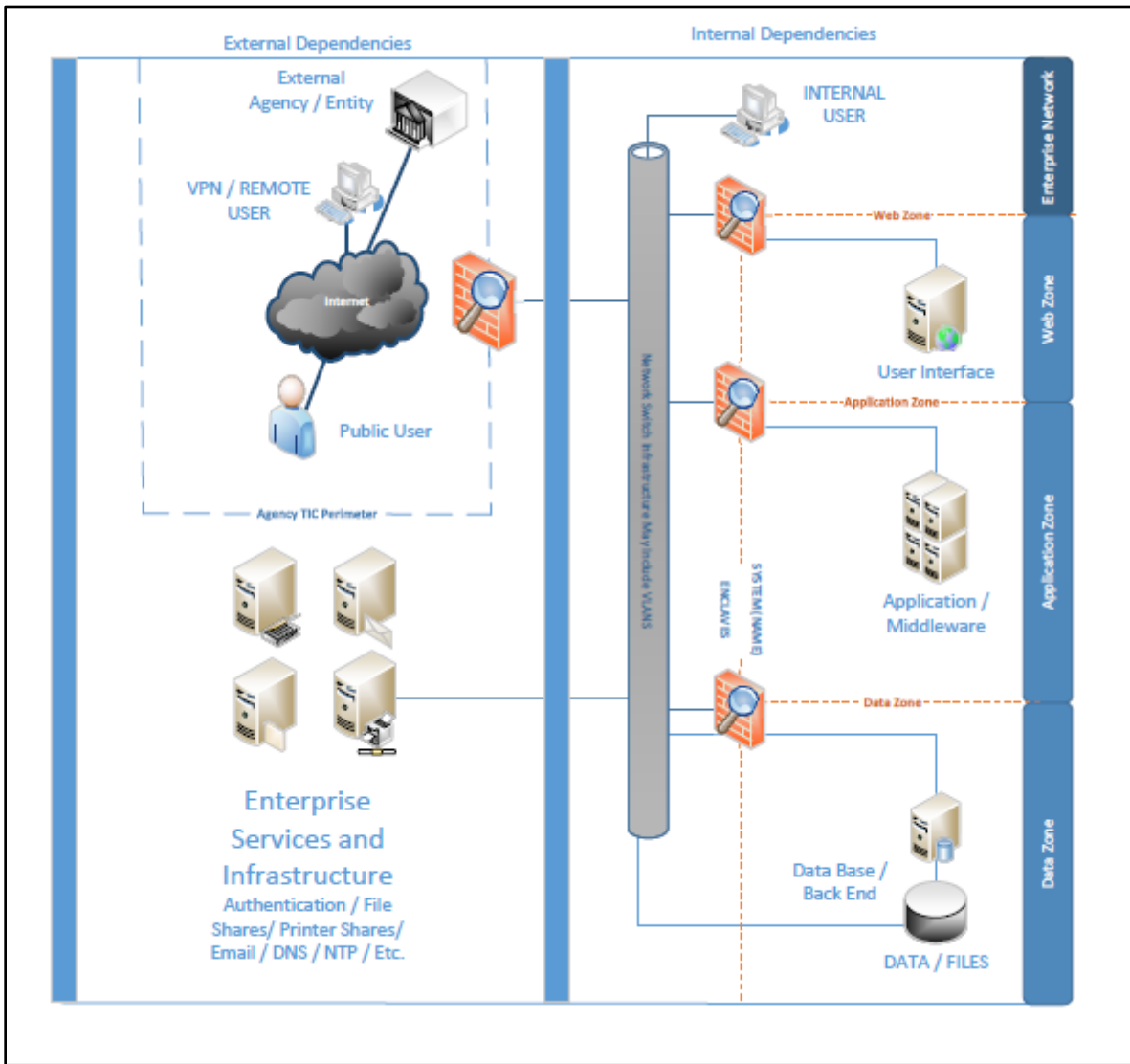
**SC-7, Control Enhancement 17, BOUNDARY PROTECTION / AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS**

Control Selection Rationale	Malicious payloads can be masked inside protocols that are authorized to traverse a HVA boundary. Often these masked packets violate industry defined protocol standards and are easily detected by boundary devices that verify protocol standards.
Supplemental Guidance	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 Plan of Action and Milestone (POA&M) processes.
References	OMB Circular A-130

**SC-7, Control Enhancement 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.
Supplemental Guidance	Isolation of HVA components limits lateral movement among those components and provides the capability for increased protection of the HVA as a whole. Additional security boundaries are to 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 is established and access controlled by boundary protection devices. As depicted in Figure 2 isolation can be facilitated using access control points to create multiple zones (web, application, and data zone). Organizations implement inspection on access control points to protect sensitive information and system components. Organizations limit access flows outbound and inspect traffic on access control points from the enclaves to protect against exfiltration of data.
Related Controls	PL-8(1)
References	OMB Circular A-130, NIST SP800-160

*Figure 3. Isolation Example*



**SC-8, TRANSMISSION CONFIDENTIALITY AND INTEGRITY**

Control Selection Rationale	Due to the sensitivity of HVA information the confidentiality and integrity of such information must be protected in transit.
Supplemental Guidance	HVA information traversing a network inside and outside the HVA authorization boundary must receive confidentiality and integrity protections. (Minimally encryption in accordance with FIPS 140-2).
Parameter Value	The HVA system protects the confidentiality and integrity of transmitted information over trusted and untrusted networks (Networks outside the HVA authorization boundary are not trusted).
Related Controls	AC-17, AU-10, IA-3, IA-8, SA-4, SC-7, SC-28
References	OMB Circular A-130, FIPS 140-2, NIST SP800-77, NIST SP800-113

**SC-18, Control Enhancement 4, MOBILE CODE / PREVENT AUTOMATIC EXECUTION**

Control Selection Rationale	Controlling automatic execution of code within the HVA protects against potentially malicious code from compromising the information, system, and mission critical services.
Supplemental Guidance	Protect the HVA by preventing the automatic execution of code on all HVA systems and system components. Example include, but not limited to, disabling auto run features on system components.
References	OMB Circular A-130

**SC-28, PROTECTION OF INFORMATION AT REST**

Control Selection Rationale	The confidentiality and integrity of HVA data must be protected for data at rest to prevent unauthorized access or exfiltration of sensitive information.
Supplemental Guidance	All data at rest receive confidentiality and integrity protections (e.g. encryption). This control applies to workstations, servers, database stores, database repositories, information stores, portable media, and share drives.
Parameter Values	The HVA system protects the confidentiality and integrity of the information at rest.
Related Controls	AC-3, AC-6, CA-7, CM-6, PE-3, SC-8, SI-3
References	OMB Circular A-130, FIPS 140-2

**SI-2, FLAW REMEDIATION**

Control Selection Rationale	HVA systems and components impacted by announced software vulnerabilities must be identified, a risk assessment performed, and remediated in accordance with organizational policies and procedures. Timely remediation of flaws is required to protect the HVA.
Supplemental Guidance	Organizations shall develop flaw remediation policies, procedures, and processes for flaw remediation that: Prioritizes flaw remediation based on vulnerability exposure and criticality risk; Defines 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; Integrate flaw remediation with change management processes; and Mitigates critical vulnerabilities on Internet facing systems in no more than 30 days. <sup>6</sup>
Related Controls	CM-6, CM-8, RA-5, SA-11, SI-3, SI-11
References	OMB Circular A-130, DHS BOD 15-01

**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.
Parameter Value	Item c1 Automatic antivirus/malware scans of all systems are completed at least bi-weekly.
	Item c2 Malicious code detection is blocked, quarantine, and the administrators alerted upon detection.
Related Controls	AC-4, CM-8, RA-5, SC-7, SC-28, SI-2, SI-4, SI-8
References	OMB Circular A-130

<sup>6</sup> DHS BOD 15-01 Critical vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems. May 21, 2015

**SI-4, SYSTEM MONITORING**

Control Selection Rationale	Monitoring the HVA to detect threats or indicators of compromise (IOC) is critical in assuring the protection of the HVA data components from compromise, loss of integrity, and loss of availability.
Supplemental Guidance	Organizations 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 is monitored for anomalous traffic, exfiltration, and indicators of insider threat. For example, a user that is copying an unordinary large amounts of information as compared to other users is identified and reviewed.
Related Controls	AC-2, AC-3, AC-4, AC-17, AU-2, AU-6, AU-9, CA-7, CM-8, PE-3, PM-7, SC-7, SI-3
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 1, SYSTEM MONITORING / SYSTEM-WIDE INTRUSION DETECTION SYSTEM**

Control Selection Rationale	System wide intrusion detection/prevention solutions provides a greater view of threats to the environment and allows for better correlation and analysis of incidents.
Supplemental Guidance	Organizations 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.
Related Controls	CM-6
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 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 inspect encrypted traffic to ensure that the traffic is legitimate and not exfiltration of data.
Supplemental Guidance	Organization balance the need for encrypted traffic verses inspection of the traffic. Organizations determine the best approach to mitigating the risks associated with encrypted traffic. Examples include but not limited to: Choose 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.
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 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.
-----------------------------	---

Supplemental Guidance	Organizations 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.
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 13, SYSTEM MONITORING / ANALYZE TRAFFIC AND EVENT PATTERNS**

Control Selection Rationale	Analyzing and profiling regular traffic and user action patterns provides a baseline that is used to detect unusual activities, traffic, or events that could indicate a compromise of information or threat to the system.
Supplemental Guidance	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. Continue to monitor traffic in these same locations and use the baselines as a comparison to detect for unusual traffic and to configure detection monitoring tools with these baseline characteristics to alert on threshold values.
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 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.
Parameter Value	Monitor and inspect outbound communications traffic at the HVA authorization boundary and at strategic locations inside the boundary to detect covert exfiltration of information.
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 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.
Supplemental Guidance	Organizations implement additional monitoring of privileged user account actions based on established policies. Organization 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.
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 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.
Supplemental Guidance	Organizations define authorized network services and implement solutions to detect unauthorized network services on the network and create alerts when

	detected. Example include but not limited to: Peer-to-peer communications, IRC, etc.
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

**SI-4, Control Enhancement 23, SYSTEM MONITORING / HOST-BASED DEVICES**

Control Selection Rationale	System wide monitoring provides a greater view of threats against the environment and allows for better correlation and analysis of incidents.
Supplemental Guidance	Implement individual host-based monitoring tools and solutions on capable devices within the HVA accreditation boundary.
Related Controls	SC-7(12)
References	OMB Circular A-130, NIST SP800-61, NIST SP800-92, NIST SP800-137

## ENTERPRISE CONTROLS

Most if not all organization’s HVAs rely on support systems and network infrastructures to provide services and solutions to the HVA environment. These components are typically part of the organizations enterprise architecture or IT service delivery platform. This dependency must be considered when assessing and addressing risk to the HVA.

For example if an organization’s HVA is dependent on the enterprise identification and authentication solution to control access to the HVA environment and that solution becomes unavailable, the HVA would also become unavailable. Organizations must ensure that enterprise dependencies for the HVAs provide the same level of assurance in protection and availability as required by the HVA.

The following controls are implemented at the organization’s enterprise level to ensure commensurate protection of HVAs. HVAs may inherit additional overlay controls from Enterprise that require further strengthening of those controls at the enterprise level in accordance with the Overlay as specified in the previous section.

### **AU-6, Control Enhancement 3, AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATE AUDIT REPOSITORIES**

Control Selection Rationale	Correlating audit records across organizational-wide audit repositories allows for better situational awareness and enterprise risk management of HVA information and systems.
Supplemental Guidance	Manage enterprise risk by correlating audit logs and events from all organizational systems to form a single risk view of the enterprise. Audit data collected at the system level (Tier 3) <sup>7</sup> shall 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).
Related Controls	AU-9
References	OMB Circular A-130, NIST SP 800-137, NIST SP 800-37 R1 & R2

### **AU-6, Control Enhancement 4, AUDIT REVIEW, ANALYSIS, AND REPORTING / CENTRAL REVIEW AND ANALYSIS**

Control Selection Rationale	Central review and analysis of audit records and events from all repositories provides improved situational awareness and quicker reactions to incidents.
Supplemental Guidance	Organizations provide capabilities that allow central review and analysis of audit records and events for all components.
Related Controls	AU-2, AU-9
References	OMB Circular A-130, NIST SP 800-137

### **AU-6, Control Enhancement 5, AUDIT REVIEW, ANALYSIS, AND REPORTING / INTEGRATED ANALYSIS OF AUDIT RECORDS**

Control Selection Rationale	The correlation of audit record information with vulnerability, performance data, and/or system monitoring information provides enhanced capabilities to identify threats, inappropriate actions, or unusual activities.
-----------------------------	--

<sup>7</sup> NIST SP800-37 R1 & R2



Supplemental Guidance	Organizations integrates audit records (from one or more: vulnerability scanning; performance data; system monitoring) into a central repository for analysis, parsing, and correlation of events to detect threats, inappropriate, or unusual activities.
References	OMB Circular A-130, NIST SP 800-137

**CP-8, Control Enhancement 5, TELECOMMUNICATIONS SERVICES / ALTERNATE TELECOM 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.
Supplemental Guidance	Alternate telecommunications testing ensures that if the alternate connection is needed it will function as expected. It is recommended that organizations fail over to the alternate telecommunications, if possible, and operate using the backup connection as part of the testing.
Parameter Value	Organizations test alternate telecommunication services at least every 6 months.
References	OMB Circular A-130; NIST SP800-34

**IR-4, Control Enhancement 4, INCIDENT HANDLING / INFORMATION CORRELATION**

Control Selection Rationale	Attacks on an organization are often targeted at multiple systems requiring correlation of information across the enterprise to promote the timely identification of threats.
Supplemental Guidance	Organizations correlate incident threat information and incident response activities across the enterprise. Correlation information must be protected at a level congruent with the highest level of information it contains (AU-9).
Related Controls	AU-9
References	OMB Circular A-130, NIST SP800-61

**PM-7, ENTERPRISE ARCHITECTURE**

Control Selection Rationale	HVAs operated in an unsegmented environment are subject to lateral compromise from adjacent systems that can be at a higher risks and are less protected. Enterprise architecture must be up to date to reflect the protection needs of the HVA to ensure an adequate level of protection for the HVA extends to the enterprise.
Supplemental Guidance	<p>The dependency of the HVAs on the enterprise mandates the integration of security requirements and controls into the Enterprise Architecture (EA) to ensure that 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 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.</p> <p>The EA is 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 incorporates agency plans for significant upgrades or replacements of legacy applications,</p>

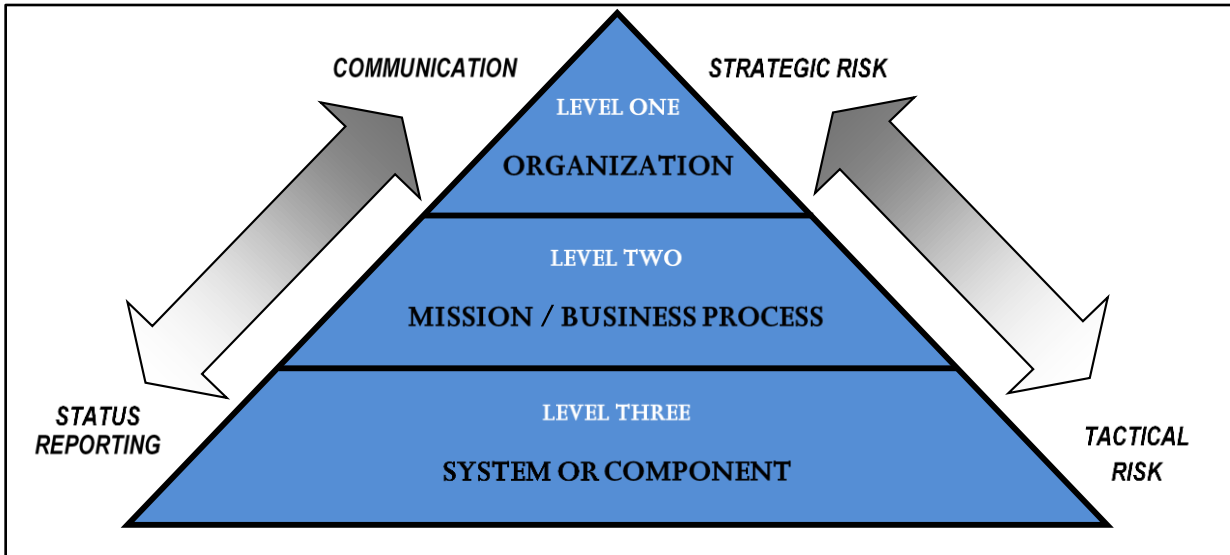
	<p>systems, or solutions that are too costly to operate, maintain, and secure. The EA includes plans for disposition of applications, systems, or solutions when no longer effectively support missions or business functions. EA includes strategies for interacting and connecting to external systems and environments (cloud, hosting providers, other government entities, contractor facilities).</p> <p>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.</p>
References	OMB Circular A-130

**PM-9, RISK MANAGEMENT STRATEGY**

Control Selection Rationale	<p>HVAs are accounted for in the strategic enterprise-wide view of risk maintained by the organization to ensure changes to the enterprise do not create unknown and unacceptable risks to the HVA.</p>
Supplemental Guidance	<p>The enterprise risk management strategy includes a process to evaluate all risks to HVA information and mission critical services. Per OMB M-17-09: “HVA risk assessments should incorporate operational, business, mission, and continuity considerations.” Organizations develop an enterprise wide risk management strategy that includes is holistic and integrated into the three-levels of the organization. Figure 3 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<sup>8</sup>. At a minimum organizations: 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 enterprise architecture. (PM-7)</p>
References	OMB Circular A-130, NIST SP800-37 R1, NIST SP 800-160

*Figure 4. Enterprise Risk Management Approach*

<sup>8</sup> NIST SP800-39



**PM-10, AUTHORIZATION PROCESS**

Control Selection Rationale	The authorization process for HVA is the primary means to identify and characterize risks to the HVA and therefore must follow a sound, documented and well-understood approach that meets the protection needs of all stakeholders.
Control Extension	Ensure an enterprise-wide perspective of both the risks posed by HVAs and the related organizational responsibilities as part of the authorization process.
Supplemental Guidance	Ongoing authorization (OA) is highly 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. <sup>9</sup> OA requires that agencies have a fully implemented Information Security Continuous Monitoring (ISCM) program as defined in NIST SP800-137. Additionally, agencies should leverage Continuous Diagnostics and Mitigation (CDM) tools and methods to automate collection, review, and alerting requirements of OA where possible. <sup>10</sup>
Related Controls	CA-6, CA-7, PM-9

**PM-12, INSIDER THREAT PROGRAM**

Control Selection Rationale	Malicious insiders are a serious threat to organizations and necessitates planning and policies to address this threat.
Supplemental Guidance	Given the sensitivity of the HVA, organizations develop and implement an insider threat program in accordance with Office of the Director of National Intelligence (ODNI) National Insider 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

<sup>9</sup> NIST SP800-137

<sup>10</sup> CDM and the Risk Management Framework

	malicious insider threats actions (DLP, monitoring, access controls, etc.) and provide insider threat training to all employees and contractors.
References	OMB Circular A-130, National Insider Threat Policy and the Minimum Standards, ODNI

**SI-4, Control Enhancement 16, SYSTEM MONITORING / CORRELATE MONITORING INFORMATION**

Control Selection Rationale	Correlating information enterprise-wide allows for comprehensive situational awareness of the security of the enterprise and potential threats and attacks to systems.
Supplemental Guidance	Organizations correlate monitoring information from enterprise monitoring tools and mechanisms such as, but not limited to: antivirus monitoring, IDS, IPS, logging, etc. Organizations must protect this information at an appropriate level congruent with the highest level of information contained within.
References	OMB Circular A-130

## **ADDITIONAL REFERENCES**

The Office of the Director of National Intelligence (ODNI), Presidential Memorandum: National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs. [https://www.dni.gov/files/NCSC/documents/nittf/National\\_Insider\\_Threat\\_Policy.pdf](https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf)

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002 & Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014

The Clinger-Cohen Act of 1996 (Pub. L. No. 104-106)

Federal Records Act (P.L. 90-620), as amended, (44 U.S.C. §3301)

Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106,

*Designation of Public Trust Positions and Investigative Requirements* (5 C.F.R. 731.106)

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

OMB Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000 & revision to OMB Circular A-130 *Managing Information as a Strategic Resource*, July 2016

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

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

Office of Management and Budget Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP)*, October 2015

Office of Management and Budget Memorandum 17-09, *Management of Federal High Value Assets*, December 2016

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

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

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

National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

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

National Institute of Standards and Technology Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006

National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012

National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010

National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, February 2010

National Institute of Standards and Technology Special Publication 800-46, Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, July 2016

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002

National Institute of Standards and Technology Special Publication 800-53, Revision 5, Pre-release - DRAFT, *Security and Privacy Controls for Systems and Organizations*, Pre-release

National Institute of Standards and Technology Special Publication 800-60, Volume II, Revision 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008

National Institute of Standards and Technology Special Publication 800-61 R2, *Computer Security Incident Handling Guide*, August 2012

National Institute of Standards and Technology Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017

National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005

National Institute of Standards and Technology Special Publication 800-92, *Guide to Security Log Management*, September 2006



National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008

National Institute of Standards and Technology Special Publication 800-132, *Recommendation for Password-Based Key Derivation Part 1: Storage Applications*, December 2010

National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011

National Institute of Standards and Technology Special Publication 800-150, *Guide to Cyber Threat Information Sharing*, October 2016

National Institute of Standards and Technology Special Publication 800-160, *Systems Security Engineering*, November 2016

National Institute of Standards and Technology Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015

National Institute of Standards and Technology Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, January 2014

Intelligence Community Standard 500-27, *Collection and Sharing of Audit Data* (June 2011)

Intelligence Community Standard 700-2, *Use of Audit Data for Insider Threat Detection* (June 2011)

Department of Homeland Security (DHS) Binding Operational Directive (BOD) 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*, May 21, 2015

Continuous Diagnostics and Mitigation: CDM and the Risk Management Framework, DHS FNR, February 18, 2016, [https://www.us-cert.gov/sites/default/files/cdm\\_files/LCE-2\\_MeetingSummary.PDF](https://www.us-cert.gov/sites/default/files/cdm_files/LCE-2_MeetingSummary.PDF)