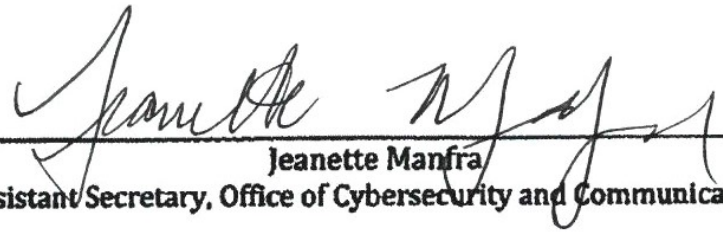
# SECURING HIGH VALUE ASSETS

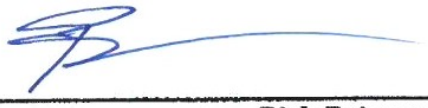
Office of Cybersecurity and Communications
Federal Network Resilience Division

July 2018

# APPROVAL TO PROCEED



Jeanette Manfra
Assistant Secretary, Office of Cybersecurity and Communications



Rick Driggers
Deputy Assistant Secretary, Office of Cybersecurity and Communications

Mark Kneidinger
Director, Federal Network Resilience Division

John Felker
Director, National Cybersecurity and Communications Integration Center

Martin Gross
Director, Network Security Deployment

# TABLE OF CONTENTS

# 1. INTRODUCTION

High value assets (HVAs) are "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." HVAs enable mission-essential functions and operations, provide services to citizens, generate and disseminate information, and facilitate greater productivity and economic prosperity.

Agencies are responsible for the information technology (IT) assets and the personal information entrusted to their organizations by hundreds of millions of Americans. A strategy that frames, assesses, responds to, and monitors risk to HVAs is thus essential. Such a strategy needs to prevent compromise and loss of data, as well as disruption of critical services and operations involving HVAs.

Recognizing the urgency, the Office of Management and Budget's Cybersecurity Strategy and Implementation Plan (CSIP) issued guidance requesting agencies to "identify their HVAs and critical system architecture in order to understand the potential impact to those assets from a cyber incident, and ensure robust physical and cybersecurity protections are in place." To provide further technical guidance on securing HVAs, the Department of Homeland Security (DHS) developed an HVA Overlay that provides security control specifications to increase the level of assurance that HVAs are adequately protected. This practice guide expands on the HVA Overlay and the CSIP's technical guidance by offering additional contextual detail and practical hardening recommendations for HVAs.

## 1.1. Relevant Agencies and Mission Areas

The technical guidance in this practice guide applies to all federal agencies, including all Chief Financial Officers (CFO) Act agencies that are required to report HVAs and ensure that cybersecurity protections are in place and functioning.

## 1.2. Rationale

The Office of Management and Budget (OMB) Memorandum M-17-09, Management of Federal High Value Assets, directs agencies to "identify, categorize, and prioritize HVAs," report HVAs to DHS annually, and ensure appropriate protections improve HVA security postures. Lessons learned from previous HVA data calls and prioritization activities show that agencies need help in understanding the architectural weaknesses within their HVA systems. In addition, "although federal guidance, initiatives, and services exist, agencies want additional help to protect their high-impact systems."

In response, the National Cybersecurity Center of Excellence (NCCoE) used findings from previous DHS assessments, and, with this practice guide, offers organizations contextual technical guidance for securing and protecting HVAs within the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

The RMF is the required framework for improving cybersecurity and strengthening the risk management process for IT systems and assets, including HVAs. In addition, the RMF enables agencies to link their risk management strategy to tactical implementation and compliance with the Federal Information Security Modernization Act of 2014 (FISMA), Federal Information Processing Standard (FIPS) Publication (FIPS Pub) 199, and FIPS Pub 200. Using the RMF, agencies can assess their HVAs, considering impact that goes beyond compliance and accounting for changing technologies as well as new threats and vulnerabilities. As a result, agencies will be more effective in

selecting and implementing the security controls needed for events such as network breaches, data loss, and HVA system downtime.

This guide also assumes that agencies have begun to develop information security continuous monitoring (ISCM) programs. ISCM programs, of which the DHS Continuous Diagnostics and Mitigation (CDM) Program is a significant component, monitor HVAs while supporting administrative and governance structures as well as use of existing contract vehicles to support remediation and modernization projects. Many of the actions this guide recommends apply to all assets within the scope of an ISCM program, not only to HVAs. Conversely, without an organized ISCM program, these actions are difficult to undertake consistently across an entire agency.

# 2. COMMON FINDINGS FROM HVA AGENCY ASSESSMENTS

## 2.1. Introduction

This section presents findings from previous HVA Agency Assessments conducted by DHS. Each finding area provides examples of issues and challenges related to implementing and maintaining robust security capabilities to protect HVAs. Section 3 then suggests techniques to address these challenges.
Organizations that already have plans to upgrade legacy environments, implement solutions or address these issues[i] should ensure that they have considered the issues the finding areas highlight or modify their plans based on the relevant guidance in Sections 3 and 4.

## 2.2. Finding Area 1 – Enterprise Risk Management

Risk management is fundamental to an organization's ability to make informed decisions to minimize the impact of system vulnerabilities. However, system owners may place operational considerations ahead of information security, thereby impacting an organization's ability to manage risk to all systems. For example, common findings from DHS assessments report risk decisions for individual systems that do not align with an organization's risk tolerance,[ii] failure to conduct system risk assessments,[iii] and failure to assess IT contractors and partners who are responsible for protecting organizational systems.[iv]

Section 3.2 provides technical guidance for the following actions:

- improving risk management with recommendations on applying the RMF
- identifying threats and business impacts
- clearly defining HVA boundaries
- exchanging information and connecting with external systems
- examining organization-wide information security program plans in the context of program management controls
- auditing systems
- security control inheritance

## 2.3. Finding Area 2 – Patch Management

The lack of continuous and timely patch management is a systemic issue for organizations. According to Government Accountability Office (GAO) Report 16-501, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, "up-to-date patches were not always installed to support selected systems where patches were available." Organizations face various challenges with patch management, including:

- difficulty identifying patches due to inconsistent documentation among vendors regarding which patches to apply to specific vulnerabilities and platforms
- difficulty coordinating patch installations due to varying release schedules among vendors, which increases complexity and causes confusion for organizations
- difficulty coordinating patch installations due to the overwhelming number of patches supplied by vendors (i.e., those released for vulnerabilities other than those being addressed)
- inadequate technology and processes that cause service and system outages during patch installation and test (e.g., auto update mechanisms for installing patches that are disabled or ignored to avoid interruptions in service or unintended impacts to the system or application)
- prioritization and limited resources at an organization to properly test and implement patches;
- limited capability to discover missing patches within systems
- contract limitations in service level agreements with vendors, system operators, and maintainers

Section 3.3 provides technical guidance addressing patch management issues.

## 2.4. Finding Area 3 – Malware Defense and Anti-Phishing

Defense against malware and vectors, such as phishing, is an ongoing challenge for organizations for the following reasons:

- Automatically identifying malware is difficult, as attackers are increasingly sophisticated about hiding malware and evolve their techniques in ways that are difficult, if not impossible, to adapt to and anticipate.

- Phishing emails are increasingly sophisticated, as adversaries are taking increasing care to craft email headers and content to appear genuine.

- Trust of email senders, document authors, and website owners is harder to establish, as collaboration with an increasing number of third parties (e.g., individuals, companies, websites, external libraries of code, etc.) means there is less time available to develop trust relationships with every person/system/resource relied upon, increasing the risk of an adversary inserting malware into the enterprise.

Section 3.4 provides technical guidance addressing these malware and phishing issues.

## 2.5. Finding Area 4 – Access Controls

Access control weaknesses continue to be an issue for organizations. According to GAO Report 16-501, agencies often do not always implement access controls effectively. The report notes, “administrators sharing accounts for authenticating to servers, rather than using unique accounts for accountability” and “systems not being configured to log all key security events to identify inappropriate or unusual activity.” Additional issues related to access controls include:

- users provisioned across different repositories with different digital identities
- user identities and access rights that remain active after the job function changes or employment is terminated
- failure to conduct comprehensive auditing, correlation, and monitoring from user access points to and beyond applications with access to data

Section 3.5 provides technical guidance addressing access control issues.

## 2.6. Finding Area 5 – Authentication

Key factors in protecting an enterprise's information assets are clearly identifying who is on a network, and only allowing authorized users to access resources. The CSIP calls for multifactor authentication using smart cards, and it specifically mandates the use of Personal Identity Verification (PIV) cards for privileged and regular users. PIV card authentication involves the use of public key (PK) technology and a public key infrastructure (PKI). Organizations face challenges in implementing strong authentication and conforming to the CSIP, including:

- level of effort required for public key enabling (PK-enabling) the applications to support authentication using standard digital certificates (e.g., X.509)
- authentication support for legacy applications where PK-enabling is not an option

Section 3.6 provides technical guidance addressing these authentication issues.

## 2.7. Finding Area 6 – Network Segmentation

Properly implementing network segmentation continues to be an issue for organizations, even though it is a known fundamental best practice for limiting adversary movement and the spread of malware, and for isolating critical data within an organization. Issues include:

- difficulty managing and keeping segmentation policies up-to-date as the network grows in terms of users and assets. In a large network, policy enforcement points can be spread across multiple areas; these need to be updated whenever a change occurs and then incorporated into the change management process
- implementing a flat network structure to avoid potential connectivity issues with certain groups (e.g., third-party vendors, cross-functional departments)
- lack of resources for the planning, implementation, maintenance, and frequent adjustments needed to deploy network segmentation zones, rules, and restrictions

Section 3.7 provides technical guidance addressing network segmentation issues.

# 3. TECHNICAL GUIDANCE

## 3.1. Introduction

The technical guidance in this section maps to the finding areas discussed in Section 2 and is organized around the Cyber Security Framework (CSF) core functions – Identify, Protect, Detect, Respond, and Recover:

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services impaired due to a cybersecurity event.

The CSF further breaks down these functions into categories and subcategories that provide organizational security outcomes and activities. To help with mapping between this document and the CSF, references to CSF categories and subcategories are ***bolded and italicized***.

## 3.2. Risk Management

OMB has directed agencies to use "a strategic enterprise-wide view of risk" to address HVAs. Consequently, the scope of HVA information system risk assessments should incorporate factors from OMB Memorandum M-17-09, *Management of Federal High Value Assets*. Risk assessment includes risk identification, analysis, and evaluation. While risk appetite and risk tolerance levels may already be set for an organization, the tolerance levels for HVAs may be more restrictive.

The following subsections discuss guidance for HVA risk management and, if applicable, reference CSF aspects (categories and subcategories) that apply specifically to risk management. Risk Management Framework

***ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.***

The RMF "links risk management processes at the information system level to risk management processes at the organization level." Further, the RMF "incorporates information security and risk management activities into a single process."[v] When agencies make risk management decisions for HVAs using the RMF, they base those decisions on their organization's and stakeholders' risk tolerance.

The RMF's six steps—Categorize, Select, Implement, Assess, Authorize, and Monitor—build upon one another, but the steps need not be implemented sequentially or hierarchically. As a lifecycle approach to ensure that the right security controls are in place to mitigate risk, the RMF, like the information systems it supports, does not enter or complete the life cycle in a linear fashion; rather, it is iterative, recursive, and non-linear.

It is essential that agencies document the decisions they make at every step of the system's life cycle (e.g., design tradeoffs, controls tailoring, not implementing certain selected controls); these decisions affect the level of risk and are critical to ensuring that the authorizing official (AO) understands the risks. **(*Reference: ID.RM-2: Organizational risk tolerance is determined and clearly expressed.)*** Thus, organizations need to bring together stakeholders authorized to consider and assume risk and determine the impacts of unauthorized access to, use of, disclosure of, modification to, or destruction to HVAs. The purpose of the RMF is not compliance with a checklist; rather, it aims to enable agencies to understand and effectively manage (i.e., frame, assess, respond to, and monitor) risk.

### 3.2.1. Scenarios

***ID.RA-4: Potential business impacts and likelihoods are identified.***

***ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.***

Organizations should employ scenario-driven or case study approaches to risk assessment for RMF decisions. Using scenarios is an industry best practice,[vi] a suggested way to conduct risk assessments (NIST SP 800-30 r.1), and one of the "variety of techniques" (NIST SP 800-39) that can be used for risk assessments. Industry experts note three major benefits of using scenarios to understand risk and opportunity:

- Scenarios encourage people to think broadly about potential outcomes, thereby preparing them to respond to a range of possibilities.
- Scenarios may reveal unexpected outcomes.
- Scenarios encourage a free exchange of ideas, protecting against group think.

Scenarios based on historical data or developed using theoretical analysis or subject matter expert input can help organizations identify risk sources, events, causes, and consequences associated with HVAs. Additionally, scenarios let organizations incorporate operational, business, mission and continuity considerations into HVA risk assessment, because a scenario can be scoped to include all levels of the organization's and stakeholders' interests. After identifying risks, organizations can analyze the nature and level of each risk and compare the results against risk criteria, to determine whether or not the risk is tolerable to the organization and its stakeholders and to develop a risk management strategy in line with their risk appetite and tolerance.

Scenario-based risk analysis facilitates understanding and response to system vulnerabilities at technical, business, and strategic levels. HVA risk scenarios should be developed with input from all levels of the organization and its stakeholders to ensure the scenarios are relevant, probable, and linked to the business/organizational and strategic objectives.

In general, a scenario should include the following components:

- actor (Who poses a threat? What is the actor's motivation?)
- threat (e.g., Was it human error, a natural event, or a malicious act?)
- event (What happened?)
- asset/resource (Was it a technical asset or a non-technical asset?)
- time (When did the event happen, how long did it last, and how long did it take to detect it?)
- potential strategic, legal, and reputation impacts

Scenarios should represent the kinds of events that could occur, but they should not be overly complex. Further, organizations should use scenarios that include the possibility of negative and positive outcomes. For example, if a scenario describes an identified vulnerability and the organization establishes backup procedures to ensure key HVA business data is always retained at a second location, the scenario outcome would be positive. On the other hand, if the organization did not put processes in place to ensure adequate backups, or if the response failed, loss or destruction of data could occur.

### 3.2.2. Vulnerability and Threat Environment

***ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.***

Organizations should be able to identify HVA system vulnerabilities, remediate those vulnerabilities to bring the HVA system in line with the organization's and stakeholders' risk tolerance, and track and monitor remediation efforts to ensure timely resolution of risks, with the highest priority risks remediated first. A risk assessment incorporates threat and vulnerability analyses to help organizations identify threats that can exploit vulnerabilities to create undesirable impacts to HVA data (e.g., unauthorized access, compromise, theft, destruction), and risk mitigation options to reduce risk to an acceptable level.[vii]

Knowledge of threat source capabilities should be coupled with discernment of a threat source's intent and targeting, or potential range of effects. For HVAs specifically, in addition to clearly understanding the impact on the system and data, organizations and stakeholders should be able to define if or why the HVA system data and information is valuable to the threat source, and what the threat source's interest is in the organization's mission and business processes. However, even without known or explicitly assumed threat intent, protections are still selected based on an assumed level of threat source capability, intent, and targeting (for adversarial threat sources), or potential range of effects (for non-adversarial threat sources).

The results of these threat and vulnerability analyses to inform risk assessment scope, security control selection, and tailoring (including security control inheritance).

### 3.2.3. HVA Boundaries

***PR.IP-7: Protection processes are continuously improved.***

Risk to a system can be imposed from outside the defined system boundary, for example, through information exchange and connections to systems and networks outside the system owner's control. What should be included within the risk assessment scope depends upon the system's size and complexity, and the organization's risk tolerance. A recommended first step for defining the risk assessment scope is to review the system's concept of operations, if it is available, or at least a detailed system description and/or system and interconnectivity diagram. Some recommended questions to facilitate scoping decisions include:

- Does the HVA system boundary fall within one authorization boundary or organizational boundary?
- What does your organization include within the HVA boundary? Why did your organization include what you have selected within the HVA boundary?
- How complex is the system (e.g., are there multiple owners, second- and third-degree interconnections, reliance on other systems)?
- Are there indications that the HVA boundary is too complex (e.g., information flow, architecture, and/or interfaces and connections are not well understood)?
- Does the HVA system exchange information with other systems, and what is the trust relationship that establishes a level of confidence that those external systems provide adequate protections?
- What risk will your organization's senior leaders accept inside the HVA boundary?
- What risk will your organization's senior leaders accept from outside the HVA boundary?
- What is the impact level of the information processed, stored, or transmitted within the HVA boundary?
  - Does the system process, store, or transmit privacy information?
  - Is the information subject to any additional protection requirements by law, regulation, or policy?
- If an incident happens within the HVA system boundary:
  - Will your organization be aware and understand what is happening within the boundary?
  - Will your organization understand if/how the incident or breach impacts the HVA?
- If an incident happens outside the HVA system boundary:
  - Will your organization be aware and understand what is happening outside the boundary?
  - Will your organization understand if/how it impacts the HVA?

#### 3.2.3.1. Information Exchange and System Connections

***ID.AM-3: Organizational communication and data flows are mapped.***

An HVA likely exchanges information with or is connected to one or more systems within the agency enterprise, at another government agency, or external to the government. In these cases, the HVA may be at risk of an attack that is initiated through one or more of its interconnections. Interconnections that are established to support HVA data communications should be configured in accordance with FIPS 140-2 and current TLS standards and specifications. Additional scoping questions are listed below.
Before accepting an interconnection, ask the following questions:

- Is the information exchange or system connection authorized, who authorized it, and has the assessment and authorization documentation been reviewed?
- To what degree does your organization's system rely on the connected system?
- Which security controls are implemented and effective on the connected system?
- Does your organization incur additional obligations to the connected system owner based on the information exchange and system connection security agreement? That is, can your organization's system impose risk on the connected system?

- Do the plans of action and milestones (POA&Ms) indicate the information exchange or connection introduces additional risk to both sides that needs to be assessed? Conversations with the other system owner(s) are necessary to determine categorization and/or classification of the system and the information exchanged.
- How do information exchange and system connections impact the level of risk to an HVA?
- What is the risk that information exchange and system connectivity and interdependencies can lead to significant adverse impact on the functions, operations, and mission of other organizations?
- Should the concerns over the connection extend the scope of the risk assessment?

Each connection must be documented. Organizations should use an Interconnection Security Agreement to specify the technical and security requirements needed to establish, operate, and maintain the interconnection. A Memorandum of Agreement is used to define the purpose of the interconnection, identify authorities, specify the responsibilities of both organizations, and define additional terms of the agreement.[viii]

Another recommendation is that organizations integrate external stakeholders (users or other interconnected systems) into the risk management process to ensure that interconnection concerns are incorporated into risk management decisions. One way to do this is to use a joint approval board to support the connection approval process.

### 3.2.4. Organization-Wide and System-Level Controls

Organization-wide security controls (i.e., in the [cybersecurity] Program Management [PM] family of controls in NIST SP 800-53) and system-level controls work together to mitigate risk. It is incumbent upon the organization to fully implement an organization-wide information security program founded on PM controls. Properly implementing the PM controls provides individual systems organization-wide with the necessary programmatic security and effectively eliminates silos. In addition, information security personnel at the individual system level need to understand that PM controls frame the approach and complement the security controls used to develop the security plans for individual information systems. PM controls focus on the programmatic, organization-wide security and privacy requirements independent of any system, and they are essential for managing security and privacy programs. Since PM controls are organization-wide, they are foundational for systems. For example, when an individual information system security architecture is developed (PL-8), it should be consistent with the enterprise architecture defined by the organization (PM-7). Individual system risk assessment (RA-3) and security assessment and authorization (CA-1) should follow the organization-wide risk management strategy (PM-9) and the Security Authorization Process (PM-10). Where applicable, each PM control specifies related controls that should further assist system-level personnel to close the gap between security controls and PM controls.

Organizations may have the impression that PM controls and system-level controls are independent of each other. As a first step, organizations should determine if they have met the PM controls, and how. One suggestion is to create a common PM control catalog (PM-1) that can be shared with the system-level personnel. The catalog should explain what the organization has done to implement the control, where any detailed information about the control can be found, *and* what the system-level (or process-level) personnel need to do at their level (if anything) to inherit the control.

Concurrently, organizations should provide organization-wide education on the information security program and show how "the security plans for the individual information systems and the information security program cover the totality of security controls employed by the organization."[ix] Another point to emphasize is that without the PM controls, the individual systems would be responsible for creating a certain level of their own programmatic security, which in turn could unnecessarily expend resources and create silos. A siloed approach can cause conflict between individual systems, as each system needs to do the same thing, but may end up doing it differently.

Additional recommendations:

- Properly designate the senior agency information security officer in accordance with FISMA, and define responsibilities within the organization to ensure that the chief information security officer has the authority necessary to execute an organization-wide security program.
- Ensure that POA&Ms are reviewed, updated, and signed off as specified in the HVA Control Overlay to track and monitor system risks.[x]
- Clearly define the membership, roles, and responsibilities of personnel within the organization performing the risk executive (function), including agency heads per Executive Order 13800. NIST SP 800-39 describes the roles and responsibilities of key participants involved in an organization's risk management process. Consider establishing a designated group (e.g., a risk board, executive steering committee, executive leadership council)[xi] comprising subject matter experts from all levels of the organization, including a "senior agency official for records management (SAORM) who has overall agency wide responsibility for records management."[xii] Areas of expertise should include security and risk assessment in the information, personnel, and physical domains, as well as budget, privacy, and legal professionals.[xiii]
- Use the CSF to facilitate an organization-wide security management approach to bring all affected parties together to understand, manage, and express cybersecurity risk. The CSF components link business drivers to cybersecurity activities and guide the consideration of cybersecurity risks as part of the organization's risk management processes. For example, the CSF's Identify function, which includes the business environment, governance, and risk management categories, directly links to PM controls such as PM-9 (risk management strategy) and PM-11 (mission/business process definition).

### 3.2.5. Auditing

***PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.***

Auditable events are those that are significant and relevant to the HVA's security and operational environment.[xiv] If there is a change in risk to the organization, the level of auditing review, analysis, and reporting should be re-evaluated. Additional audits may be conducted upon request (i.e., after an incident, or to review audit logs to identify security incidents, policy violations, and fraudulent activity while providing information for mitigating a security event). An organization should adjust the frequency, scope, and/or depth of the audit review, analysis, and reporting when there is a change in risk based on law enforcement, intelligence, or other actionable sources of information.

***DE.AE-2: Detected events are analyzed to understand attack targets and methods.***

***DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.***

***RS.AN-1: Notifications from detection systems are investigated.***

Audit review, analysis, and reporting activities relate to system activity evaluation through the inspection of system log data. Capabilities to collect, review, and analyze audit data should include those listed below.

- Automated mechanisms to integrate audit review, analysis, and reporting processes. An organization should use integrated audit review, analysis, and reporting to support a process for investigation and response to suspicious activity so it can respond methodically to potential incidents.
- Collection and indexing tools to aggregate all audit and log records from all sources within the organization's purview of responsibility. This should include, but not be limited to, servers, client machines, sensors, network devices, directory services, virtual machines, Radio Frequency Identification, security devices, mainframes, etc. Logs should be analyzed for correlating trends and events, first instance of

notification, frequency of information, events, alerts, anomalies, etc., and deltas between logs that "should" be the same.

- Central review and analysis of audit records from multiple components within the system. This feature is critical, since an individual administrator who only observes a small subset of the environment may not recognize trends in the enterprise. Therefore, all log/event data needs to be collected in a central location where the personnel have the training, time, equipment, clearance, and access to fully review and provide sound analysis of the data.
- Integration of information from performance data, vulnerability scanning, or information system monitoring with the analysis of audit information. Correlating audit record information with vulnerability scanning information helps determine the accuracy of vulnerability scans and correlate attack detection events with scanning results.

#### 3.2.5.1. Protecting Audit Information

HVA information needs to be properly protected from unauthorized access, modification, and deletion. This applies to both initial generation and backup of audit records.

- Use of write-once media removes the possibility of an intruder or privileged user intentionally or unintentionally changing a file. A write-once backup ensures that files are in the same condition as when they were first stored. Write-once media includes Compact Disk-Recordable (CD-R), Digital Video Disk-Recordable (DVD-R), and WORM (Write Once Read Many) media. Tape cartridges or Universal Serial Bus (USB) drives are write-protected, but are not write-once media.
- An audit record backup must be physically separate from the audited system to ensure that the audit data cannot be affected, manipulated, or subjected to intentional data loss by someone who wishes to cause harm. If the separate backup is stored onsite and the organization suffers a catastrophic event such as a fire, all audit data could be lost. The proper way to store an audit record backup is on two separate systems, with one backup onsite and a second backup on a separate system at a separate location that is a safe distance from the original, onsite location (e.g., cloud, CD-R).
- It is essential that security events be written simultaneously to both the local security log and remote backup device(s), and that all users of the logged system, including the administrator(s), cannot access the remote device(s) to which the audit records are being written. This will further mitigate the chance of an insider threat going unnoticed.

Because the integrity of audit data may be compromised, audit records need to be protected from the moment they are generated and throughout their storage life. To protect the integrity of audit information, cryptographic mechanisms such as encryption hashing should be in place. For example, signed hash functions using asymmetric cryptography enable distribution of the public key to verify the information while maintaining confidentiality of the secret key used to generate the hash. Only privileged users with access to the encrypting certificate can view the audit records. Using signed audit records ensures that data modifications can be detected.

##### 3.5.2.1.1. Audit Information Access Control

An organization should specify the permitted actions for the information system process, role, and/or user associated with audit information review, analysis, and reporting. Permitted actions are enforced by the information system and include read, write, execute, append, modify, and delete. Specifying permitted actions on audit information helps reduce the information's attack surface by removing unnecessary privileges that can result in information compromise, and enforces the principle of least privilege based on a user's job necessities.

An organization should also require a distinct environment for the dedicated analysis of audit information related to privileged users. Restricting privileged user authorization to read-only helps to limit the potential of deleting audit records, either accidentally or to cover up malicious activity. In addition, the read-only feature of audit

records should be granted based on need-to-know. Dual authorization, which requires the approval of two authorized individuals to execute an action, can prevent a user from intentionally or accidentally moving or deleting audit records. The specific audit information and procedures for which dual authorization is required (e.g., movement and/or deletion of the information) should be documented, and the dual authorization requirement should be enforced. Audit entries are created when a dual authorization request is issued, approved, or rejected.

### 3.2.6. Security Control Inheritance

Common controls are those for security and privacy, which can be inherited by one or more organizational systems. Common controls can also be identified at different levels of the organization, including, for example, corporate or agency level, bureau or subcomponent level, or individual department level. Organizations identify and select the set of common controls and then assign them to organizational entities designated as common control providers.

Organizations benefit from using common controls because they "can support multiple information systems efficiently and effectively as a common capability."[xv] The individual, group, or organization designated as a common control provider (CCP) is responsible for developing, implementing, assessing, and monitoring the common control(s). Implementation details about inheritable controls should be documented in the CCP's System Security Plan or equivalent document. Weaknesses found in common controls are captured in the POA&M. This information should be available to HVA system owners using the common controls so that the weaknesses can be addressed as needed to protect the HVA.

Security control inheritance can be efficient and economical, but organizations must apply the same level of rigor to risk assessment when inheriting controls. The extent to which a system can benefit from security control inheritance depends on how many of the common controls can be inherited, and the degree to which each of those controls satisfies the system's unique security requirements. An inherited security control that does not meet the security requirements for the system and its operating environment should be supplemented to reduce the level of risk to an acceptable level, or it should be replaced by a completely different control that more fully meets the system's security requirement. For example, the physical and network security controls may meet the organization's risk tolerance; however, because the CCP is generally trying to satisfy the needs of the majority of systems that might use the common controls, the common or inherited controls may not meet the needs of an HVA system's operation. Ultimately, the CCP should be thought of as an unexpected benefit that can be accepted or supplemented; inheritance should not be viewed as an all-or-nothing approach.

Supplementing a security control can potentially increase an HVA's cost and complexity. This is a risk decision, and the cost of supplementing a security control where needed must be weighed against the cost of not doing so.

The following points should be considered regarding inheritance:

- Inheritance is not limited to the enterprise level; it can occur at or from a different part or entity within the organization that resides within the enterprise, such as a mission or business area.
- Once inheritance decisions are made, agencies conduct a risk assessment (RA) on HVAs to determine what, if any, risks may remain after CCP inheritance occurs (i.e., what is unique to protecting that HVA). To address and mitigate any risks identified by the RA, the HVA's security control set may need to be tailored or HVA specific security controls may need to be implemented. The risk assessment allows the AO to make informed, risk-based decisions, which can include the following options:
  - accept and inherit the controls as implemented along with any risk that goes with that decision
  - reject the controls entirely
  - accept the risks while determining compensating measures (logical or physical) to reduce risk to an acceptable level. HVA subsystems and/or components must be evaluated to determine if the protections/safeguards provided can be accepted and reduce the risk to an acceptable level.

It is possible for an HVA to inherit controls from a CCP with a higher or lower security categorization than the HVA itself. When an HVA inherits controls from a CCP with a lower impact level, the CCP is not required to change its impact level to meet the HVA's needs. Raising a CCP's categorization could have resource and financial impacts to cover all systems that could potentially inherit from it.

## 3.3. Patch Management

NIST SP 800-40 Rev. 3, *Guide to Enterprise Patch Management Technologies,*[xvi] describes patch management (also known as *flaw remediation*) as the "process for identifying, acquiring, installing, and verifying patches for products and systems." The following subsections discuss technical guidance for HVA patch management and, if applicable, reference CSF aspects (categories and subcategories) that apply specifically to patch management.

Overall, effective patch management involves the following actions, which are organized by CSF function:

- (Identify) identification and automated inventory updates for hardware and software on systems, and active monitoring of vendor websites, vulnerability alerting services, and threat intelligence feeds to identify new vulnerabilities and patches that may apply to systems
- (Protect) automated patch management process that is integrated with the organization's change control and vulnerability management program
- (Detect and Respond) automated and ongoing monitoring to ensure patches have been successfully deployed and the associated vulnerabilities have been remediated

### 3.3.1. Identify

A prerequisite for effective patch management is identifying and tracking system components (physical or virtual) and vulnerabilities on an organization's network. This information needs to be current and updated automatically to help determine the current patch level and which patches and updates have not been applied.

***ID.AM-1: Physical devices and systems within the organization are inventoried.***

It is necessary to identify and maintain hardware inventory to understand at a baseline level what might need a patch. To ensure that inventory data is accurate and timely enough to support the vulnerability and patch management process, it is recommended that inventory data be collected at least every 72 hours.[xvii]

***ID.AM-2: Software platforms and applications within the organization are inventoried.***

NIST SP 800-40 Rev. 3[xviii] states that "enterprise patch management is dependent on having a current and complete inventory of the patchable software installed on each host." For the purposes of flaw remediation, software includes patchable applications, operating systems, driver and Basic Input/Output System (BIOS)/firmware updates. Software inventory information is also used to determine what software is compliant and to ensure that flaw remediation (patching) requirements are met.

The following information should be collected automatically to ensure the level of granularity needed for tracking and reporting software:

- software product name
- software version number
- software patch level
- unique host device ID to link to hardware inventory

- software component file path/name
- software vendor

In addition to software component file names, collecting individual file attributes, such as file size information from product executables (e.g., .exe, .dll), helps improve visibility into the patch level of systems, since vendors often release patches that do not change the installed product version information but do update product files. In those cases, the only way to differentiate patched versus unpatched is to look at the files that were updated to fix the vulnerability.

To help ensure a current inventory of patchable software, it is recommended that inventory data be collected at least every 72 hours.[xix] This frequency ensures the inventory is validated and updated on a near-real-time basis.

HVA owners should remove unnecessary software installed on HVAs to reduce the attack surface and the number of patches for which they need to be responsible. They should also plan for replacing software or hardware nearing end of life, especially when the end of life is due to lack of vendor support (***Reference – PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition***). Monitoring with an ongoing up-to-date inventory system helps track warranties and the age of systems necessary to plan the replacement of end of life systems before they reach their expiration dates. The software asset management capability should provide alerts and reports that support end of life monitoring. NIST SP 800-64 Rev. 2 includes additional information on the disposal phase of the system development life cycle, and NIST SP 800-160 shows activities and tasks to be considered to handle replaced or retired system components.

***ID.RA-1: Asset vulnerabilities are identified and documented.***

A study that sampled 50,000 organizations showed that at approximately 40–60 days from a vulnerability's release, the probability that the vulnerability would be exploited is around 90%. However, it has also been shown that, on average, security teams take 100–120 days to remediate existing vulnerabilities. The study also noted that "security teams are (1) slower than the attackers, (2) they often remediate vulnerabilities which aren't being exploited, and (3) they're being overrun by non-targeted, automated attacks."[xx]
To address this timeline gap, organizations should prioritize vulnerabilities to ensure those that are being actively exploited are remediated first, using information from the following sources (***Reference ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources***):

- vendor and security sites to monitor news and product advisories that are relevant to the products used at the organization. The amount of information that vendors provide in their advisories can vary widely; Common Vulnerabilities and Exposures (CVE) information can provide more details to assist with the vulnerability prioritization process.
- vulnerability alerting and management services that deliver information on newly discovered security issues, vulnerabilities, and exploits
- automated near-real-time threat data feeds to determine what is being exploited at the current time, by whom, and rate of exploit, to help prioritize which vulnerabilities specifically pose a threat
- alerts from the United States Computer Emergency Readiness Team (US-CERT) which provides access to the following tools:
  - Automated Indicator Sharing – indicators of compromise and defensive measures shared in real time via Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)
  - cyber threat information sharing via DHS's Shared Service offerings, such as LookingGlass and iSIGHT Partners (free for federal partners)
  - US-CERT portal compartments (GFIRST, Mercury, Cobalt)

Based on this information, organizations can effectively categorize a vulnerability and determine how quickly it needs to be remediated.

DHS Binding Operational Directive (BOD) 15-01 states that critical vulnerabilities on internet-facing systems must be remediated in no more than 30 days.[xxi] Organizations opting for a quicker vulnerability remediation schedule can align with the following best practices:

- remediate vulnerabilities categorized as high and correlated with threat information showing the vulnerability is being actively exploited within 48 hours[xxii]
- remediate medium category vulnerabilities within one week.[xxiii] Medium category vulnerabilities refer to those that are more difficult to exploit or are currently only exploitable in theory.
- remediate low category vulnerabilities within one month

### 3.3.2. Protect

***PR.IP-12: A vulnerability management plan is developed and implemented.***

A vulnerability management plan goes hand in hand with a patch management plan to ensure timely remediation of HVA vulnerabilities. A vulnerability management process breaks patches and security bulletins down to individual vulnerabilities or CVE, while patch management is the "process for identifying, acquiring, installing, and verifying patches for products and systems."[xxiv] Both processes are needed to effectively remediate vulnerabilities on HVAs.

#### 3.3.2.1. Vulnerability Patching

How the organization remediates a vulnerability can depend on whether or not a patch is available. If a patch is not available, there should be a plan in place to mitigate the vulnerability. Example mitigation strategies include performing log analysis to look for indications of a vulnerability being exploited, whitelisting software, modifying IDS or firewall rules, and/or system isolation. This mitigation plan should also be used if a patch fails during testing.

If a patch is available, its effective and timely deployment relies on the effectiveness of the patch management process. Best practices for the patch management cycle are listed below.

- Develop and decide upon a documented flaw remediation process up front, including the workflow and approval chain for approving and testing patches, uptime requirements for the HVAs, and HVA patch window times. In addition, configure test groups in the patch management system to create representative samples of platforms for each HVA, ensuring that custom applications are included in a representative group. Create representative test groups for each type of HVA.
- Leading up to the deployment of patches, reserve system downtime and patch windows as needed. Also, ensure that patches, service packs, or hotfixes from previous patch cycles are not outstanding, since current critical patches sometimes depend on whether past non-critical patches have already been applied. In addition, some software patching cannot occur if the system is pending reboot.
- Once the patch is released, examine vendor documentation, security bulletins, email alerts, and webinars that vendors provide to understand the vulnerability addressed, the severity rating, and if there are any associated active exploits. Base severity rating and prioritization of patches on the vulnerability prioritization efforts described in Section 3.3.1 above, under the CSF subcategory ID.RA-1 reference. Use that information to prioritize patches and assess the impact and applicability of HVA patches, which will help determine which ones to send first for change control/approval, testing, and deployment.
- Over time, analyze the types of software running on HVAs and how often they get updated. Group software by how often it is updated and its importance. This analysis and categorization can help meet patch cycles,

which continue to get shorter, and with the limitations many organizations have in performing comprehensive testing for all patches. For example:
    - Group 1 – Self-Update: Software the organization allows to self-update.
    - Group 2 – Managed Deployments: Patches are deployed as soon as they are received, but with oversight of IT staff, and they are first deployed on a limited number of systems, starting with less critical or pilot systems. If no issues are identified after a set amount of time, patches are then deployed on other and more critical systems.
    - Group 3 – Formal Testing: Patches go through a testing process before being deployed to ensure that no issues occur with systems being patched. Software flaw remediation for this group uses rigorous testing within test environments to ensure business continuity of the HVA system ***(Reference – PR.DS-7: The development and testing environment(s) are separate from the production environment).*** Testing includes stress testing (transaction volume) with as many types of interactions as occur in the operational system, management function testing (administrative changes, user changes), and security testing (e.g., tests for open ports and protocols that should be blocked).
- Provision a rollback for patch management (restore to original pre-patch configuration), and retain the previous version of the baseline configuration to support rollback.
- Implement and test HVA backups to mitigate downtime that may occur during the patching process ***(Reference – PR.IP-4: Backups of information are conducted, maintained, and tested periodically)***. Test backup information by performing a restore as frequently as specified in the HVA Control Overlay.[xxv]

Finally, applying the patch does not always eliminate the vulnerability. Occasionally, system or application configuration changes are required post patching as well. Check patching and release notes for any post-patching steps required to fully protect systems.

### 3.3.3. Detect and Respond

***DE.CM-8: Vulnerability scans are performed.***

***RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.***

Vulnerability scans are performed to determine vulnerability and audit/compliance findings, and whether a system is configured in accordance with the organization's standards, baselines, and policy. For HVAs, the frequency of conducting vulnerability scans should support increased visibility of the system, decrease the time between making a fix and determining a fix was not implemented correctly or did not remediate a vulnerability, and provide more up-to-date data to correlate with other data sources, such as IDS events, or to help an incident response team. The 2016 Verizon Data Breach Investigations Report[xxvi] states that "half of all exploitations happen between 10 and 100 days after the vulnerability is published, with the median around 30 days." Therefore, conducting scans monthly, quarterly, or less frequently would result in a greater probability of vulnerabilities being exploited between an organization's scan cycles.

To align with requirements of the DHS CDM program, conduct vulnerability scans once every 72 hours.[xxvii] For vulnerabilities identified by CVE, the goal is to discover any newly introduced vulnerability within 72 hours from its introduction on the system. To identify vulnerabilities on an HVA, augment credential-based scanning with non-credential scans. Credential scans determine if a patch for a given vulnerability has been applied, verify the system configuration, determine software version installed, and identify vulnerabilities associated with a specific software version. Agent-based scans can be used in place of credential-based scanning if credentials are not available. Agent-based scanners rely on agents that are deployed to each system manually or automatically through a software management system using scripts, and are scheduled and controlled through a centralized agent manager. Non-credential scans should be used to augment and verify the credential-based scan results, and can be run multiple times per day on an HVA.

If a scan cannot be completed successfully, the scan or monitoring system should alert administrative personnel within one hour.[xxviii] Access to the vulnerability management system account should be maintained via a role-based schema for authorized users only. Updates to definitions used by vulnerability scanning tools should be applied as they become available from the vendor to ensure that assets are scanned for the latest known vulnerabilities. A standard vulnerability scanning tool will provide both regular updates and updates based on triggered events, such as when highly visible vulnerabilities are discovered.

The vulnerability scanning procedure should also be used for continuous monitoring to ensure that vulnerabilities have been successfully remediated. Post-deployment patch management should include the following actions:

- validating that any necessary reboots occurred or identifying HVAs that need a reboot to complete installation of the patch
- providing success/failure results and percent complete for the number of applicable systems
- providing return code of the individual patches to assist in investigating patching issues or identifying systems that fall into a specific failure state

## 3.4. Malware Defense and Anti-Phishing

This section discusses the CSF aspects (categories and subcategories) that apply specifically to malware defense and anti-phishing. As with all attacks, an organization needs to plan defenses to thwart the infestation of malware (CSF function Protect). The organization also should assume that sooner or later an attack will succeed, and it therefore needs to plan to Detect, Respond, and Recover from that event. The subsections below provide specific information within each subcategory to describe tools that enable the security function associated with the subcategory.

Overall, defending against malware and phishing involves the following actions, which are organized by CSF function:

- (Protect) developing activities to block phishing emails from getting into an organization, and activities to block malware from running
- (Detect) detecting phishing attempts, detecting if malware is running, and limiting the effect of any compromise by isolating the process, application, or host
- (Respond) responding to phishing attacks and stopping the immediate impacts of malware, such as data exfiltration or corruption
- (Recover) restoring HVAs lost to malware and phishing attacks, and implementing permanent changes to defend against future similar attacks

### 3.4.1. Protect

The simplest way to protect the potential victim from activating malware is to not deliver it in the first place. Mail servers can be configured with technologies such as Domain Name System (DNS)-based authentication of named entities (DANE), DomainKeys identified mail (DKIM), Domain-based Message Authentication Reporting and Conformance (DMARC), and spam filters that weed out suspicious messages before they get to the intended victim. However, email from seemingly legitimate senders can be created to get past these technologies. DRAFT NIST SP 800-177, *Trustworthy Email*, provides further details.

To check whether malware can be activated, user actions that would activate it (e.g., opening an attachment) can be emulated in a self-contained virtual environment that is not subject to harm from malware (a so-called *detonation chamber*). This can be accomplished by products that reside in the infrastructure as an enterprise service or on each endpoint for local protection. Products can provide this isolation in different ways:

- isolating the mail client or internet browser on a network segment with limited connectivity to the HVA
- isolating the application by putting a container around the mail client or browser
- isolating any attachment or Uniform Resource Locater (URL) dereference
- copying attachments to an isolated container before opening them
- isolating the applications off-site (e.g., at a cloud provider), again with limited network connections to the HVA

Messages where malware is detected should be flagged for review by a team designated to review suspicious emails and then delete them from the user's mailbox. The team can make changes to mail blocking systems or services to increase the chances that similar messages are blocked prior to delivery to users.

Another way to head off the attack is to stop the victim from activating the malware (e.g., by opening an attachment or URL). The attack's success requires the victim's active (if unwitting) participation; an attachment containing malware that is never opened, for example, is not harmful. Usually a large component of this protection is user training ***(Reference – PR.AT-1: All users are informed and trained).*** Users can be taught to be cautious when opening an attachment or URL, which can lead to fewer successful attacks. Anti-phishing products and services are also available to support user training and help identify users who do not follow phishing email awareness policies. It should be noted, however, that attackers are becoming increasingly sophisticated, and it is not unusual even for users with experience and heightened awareness to be fooled by a message.

Other options to block malware from running include those listed below.

- Services that can detect URLs embedded in mail messages that are obfuscated (and hence suspicious) or refer to known bad sites.
- Application whitelisting (AWL) software that contains a list of all allowed applications and processes, and ensures that any software not on the whitelist is not allowed to run. AWL stops malware from running if it uses a process name that is not on the list; however, it will not protect the system if the malware masquerades as an approved application or process. NIST SP 800-167, *Guide to Application Whitelisting*, provides further details.
- All network activity on the hosts should be recorded, including source Internet Protocol (IP) address and port, destination IP address and port, and session duration, to accommodate forensics if needed.
- NIST SP 800-83 Rev.1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, also provides recommendations for malware prevention in the areas of policy, awareness, vulnerability mitigation, threat mitigation, and defensive architecture.

Effectiveness of these options can be tested against historical messages to help quantify their impact before implementation.

### 3.4.2. Detect, Respond, Recover

Despite an organization's best efforts, a phishing attack will eventually succeed and malware will compromise the network. Once the malware has been installed, the remaining attack and defense activities are the same as for malware that enters the network through any other means (e.g., an infected website, DVD-R, or USB drive). In anticipation of this eventuality, the organization needs to put in place processes and technologies to detect the malware or evidence of its presence, take action to isolate and mitigate the harm, remove the malware and update the organization's protections to avoid being infected by the malware again, and recover its data and systems to a clean and known good state.

#### 3.4.2.1. Detect

***DE.CM-4: Malicious code is detected.***

An organization's sensors may detect malware based on something known about it (signature-based detection) or by inferring that it is badly behaving software (anomaly-based detection). Examples of detection are listed below.

- anti-malware software that is specifically looking for files or processes with specific names, or looking for unusual usage patterns in central processing units (CPUs), file systems, or networks
- intrusion detection systems looking for attacker use of IP addresses (e.g., for command and control) or use of unusual (including blocked) ports or unusual packet structures
- application whitelisting software that does not match the name of the malware, stops it from executing, and logs it or takes other defensive action

Specific detection activities are described below:

- installing anti-malware defenses
  - If feasible, the organization should install and configure whitelisting software. NIST SP 800-167, *Guide to Application Whitelisting*, provides more detailed discussion on application whitelisting planning and implementation.
  - If whitelisting is not used, the anti-malware defense software must include the ability to use non-signature-based (also called anomaly-based) detection mechanisms. Signature-based malware detection has known deficiencies that are too numerous to allow it to be the only defense mechanism for HVAs.
- updating software (including new signatures and detection patterns, in addition to software patches and upgrades) as soon as updates are made available, and in accordance with the organization's configuration management policy for HVAs
- configuring malicious code detection software to check every executable before it is run, and every file before it is stored. If that cannot be done, schedule scans of all systems with at least a frequency as specified in the HVA Control Overlay.[xxix]
- logging all executions of applications or libraries (e.g., Microsoft Dynamic Link Libraries [DLLs]) on execution, load, create, and terminate. When a problem is discovered, it is important to block the potentially malicious activity and send a high-priority alert about the activity to the organization's security information and event management (SIEM) system.
- determining if the malware detection software can auto-update without interfering with the HVA's functioning or availability. Auto updating is ideal because it usually leads to the least time between an update being available from the malware detection manufacturer and obtaining its improved protection for the HVA. In some cases, updates need to be checked first in a sandbox environment, or at least reviewed by a security operator before being applied, as they might interfere with HVA operation.
- ensuring that updates to anti-malware software are made only by user accounts that are specifically authorized to update the HVA's cybersecurity software. Ideally, each HVA will have its own controlling attributes so the minimum number of privileged users will be able to perform the updates (*users* in this case refers to logical personas, not necessarily to individuals).
- automatically testing the HVA's malware protection periodically and ensuring that those test results are immediately reported and reviewed ***(Reference – DE.DP-3: Detection processes are tested)***. In theory, software should be tested continuously as it runs and examines all executables and files. In practice, there are unusual cases (such as the defensive software being turned off, or the configuration being changed to not perform detection) that are best discovered by having a known, uniform, repeatable test run on a regular basis. For an HVA, testing ought to be done daily if possible, but at least weekly.
- identifying, analyzing, and characterizing detected malicious code ***(Reference – DE.AE-2: Detected events are analyzed to understand attack targets and methods).*** The HVA owner would not do this; instead, it would be done by the larger organization running the network (if it were large enough to afford to do so) or by an outside organization. For an HVA of sufficient national importance (i.e., not just an HVA to the

owning organization), analyzing the malware could return important information. Organizations should report incidents to US-CERT when appropriate (guidelines can be found at https://www.us-cert.gov/incident-notification-guidelines), because they can help analyze the malware and generate indicators of compromise that can then be provided to other organizations, so they can check if they have been victims of the same malware.

#### 3.4.2.2. Respond

***Mitigation RS.MI: Activities are performed to prevent expression of an event, mitigate its effects, and eradicate the incident.***

Ideally, most responses to malware detection will be automatic and appropriate, including the following responses:

- logging that the malware was detected
- stopping the malware from executing
- isolating the process, application, or host
- notifying the appropriate personnel
- removing the malware and affected files from victim systems

Manual or semi-automated responses are listed below.

- accelerating the application of patches that defend against the weakness the malware exploits
- instituting mitigations (e.g., temporary firewall rules) that defend against the malware by blocking access to its command and control server or blocking exfiltration of data
- checking the integrity of data and software on the HVA that may have been affected by the malware
- quarantining the impacted machine or service from any network connection, either inbound or outbound

There is also a continuity of operations aspect when responding to a malware attack. The HVA should have an expected availability requirement (including a maximum tolerable downtime requirement and accessibility from various network segments, such as from remote sites) that guides how long, if at all, the HVA can be taken offline to respond to the attack (***Reference – PR.IP-4: Backups of information are conducted, maintained, and tested periodically).*** The lower the maximum tolerable downtime, the more frequently the backup system and procedures should be practiced.

#### 3.4.2.3. Recover

***RC.RP-1: Recovery plan is executed during or after an event.***

***RC.IM-1: Recovery plans incorporate lessons learned.***

Longer term recovery actions fix any resources the malware damaged, and institute or reinforce protections or add new protections against future attempts to use this piece of malware or variants:

- recovering any data or software from trusted backups to replace those corrupted by the malware. It is important not to restore backed-up copies of the malware. Analyzing the malware and available log files can help determine how long the malware may have been resident. For additional information see NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*
- implementing permanent technology changes to replace short-term mitigations
- implementing policy and training as appropriate to complement technology solutions (e.g., refresher training on recognizing and reporting phishing attempts)

For additional information, NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, provides guidance on malware incident response in the areas of preparation, detection and analysis, containment, eradication, recovery, and lessons learned.

### 3.4.3. Example of Deployed Solution

*Figure 1* shows a generic architecture for deploying an anti-malware solution.

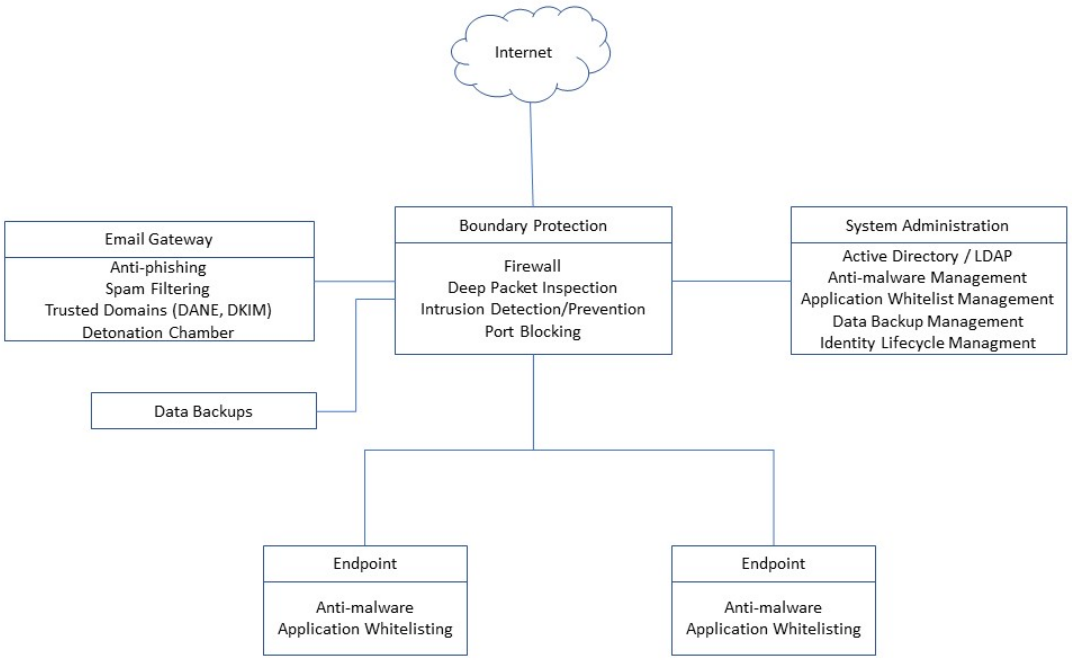



*Figure 1. Generic Architecture for Deploying an Anti-Malware Solution*

The elements of the diagram are as follows:

- Boundary Protection: This device, or collection of devices, enables the connection to the wide area network (here represented as the internet). This protection includes the following features:
  - a firewall to filter for malicious network traffic packet headers
  - deep packet inspection to look for malicious activity within the payload of packets
  - intrusion detection and/or prevention to filter for malicious IP addresses
  - port blocking to lock down ports that the whitelisted software does not need
- Email Gateway: This device, or collection of devices, handles incoming email and includes capabilities for the following items:
  - anti-phishing software to scan for messages that appear to be targeted at getting users to allow malicious software to run or to exfiltrate sensitive data
  - spam filtering software to weed out messages that the organization does not need
  - mailer configured to use standards-based means to recognize trusted domains to support filtering out unwanted or malicious messages
  - detonation chamber to test out links and attachments in messages for malicious behavior
- Backups: used to recover files if there is corruption or other problems with files on the endpoints

- System Administration: a device, or collection of devices, that allows only privileged users to make changes in administrative configuration of the network, including the following administrative components:
  - a directory (e.g., Active Directory or Lightweight Directory Access Protocol [LDAP]) and identity management capability for provisioning accounts and access permissions
  - centralized management for anti-malware, including managing updates for signatures and behavioral patterns
  - application whitelist management
  - data backup management
- Some number of endpoints, each with agents to implement anti-malware defense and application whitelisting enforcement.

## 3.5. Access Controls

Controlling who and what forms of access are allowed is key to protecting resources from unauthorized access. Implementing access control commensurate with risk is an important part of strengthening the risk posture of HVAs. The discussion in this section is primarily about logical access control. The guidance discussed here is generic; organizations can apply these controls as a starting point and augment them with additional controls specific to their HVAs.

Overall, improving access controls for HVAs involves the following actions, which are organized by CSF function:

- (Identify) establishing a governance structure by developing well-defined business processes and access control policies for who and what can access an HVA, and what roles and privileges of access are allowed
- (Protect) implementing technical solutions for lifecycle management of identities and credentials with automated approval workflows and identity governance, and enforcing access to HVAs in accordance with the organization's access control policies
- (Detect) detecting unauthorized access and non-compliance with the HVA's access control policies for provisioning and approvals by reviewing audit logs and reports generated by the provisioning and governance tools
- (Respond) addressing security incidents using the established business processes and governance structure and adjusting access controls commensurate with incident risk
- (Recover) gathering lessons learned, and reassessing and modifying the access control policies to prevent future compromises

### 3.5.1. Identify

***ID.GV-1: Organizational information security policy is established.***

***ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners.***

Establishing a governance structure for administering access control is a crucial step in controlling access to the HVAs. Applying the best technologies and solutions to control access will not be effective if there are no supporting business processes and policies in place. The information/data owners, business process experts, information security experts, privacy experts, and risk management experts should be collectively engaged to take a holistic view of the mission and data associated with each HVA, and the types of users accessing the HVAs, and they should establish the business processes and access control policies to protect the HVAs from unauthorized access. An access control policy for an HVA addresses the following aspects:

- level of assurance requirements for authenticating entities to HVAs

- Assignment of job functions to roles in the organization
- type of access rights allowed for each job function, in accordance with the principle of least privilege
- authorities responsible for approving the assignment of a privileged role to a user
- frequency for reviewing and re-approving the privileged role
- role training required for the privileged user roles and how frequently the training should be repeated
- job functions associated with the HVA for which separation of duties should be enforced
- timeframe to modify or de-provision a user's access to the HVA following a job function change or employment termination
- remote access restrictions

Some things to consider in developing the business processes are listed below.

- workflows for the approval of user access rights in accordance with the access control policies
- process involving the right authorities to modify or remove all user access rights following a human resources-related event, such as a change in job function or employment termination
- workflow for the authorized parties to approve the assignment of a privileged role to a user
- procedures and chain of command to respond and recover during a compromise or insider threat
- process to ensure that partner organizations, if any, follow equivalent security practices

## 3.5.2. Protect

### 3.5.2.1. Access Control

***PR.AC-1: Identities and credentials are managed for authorized devices and users.***

A large and crucial part of implementing strict access control involves proper lifecycle management of the digital identities, credentials, and access rights for the entities accessing the resources. It is common for organizations to find users provisioned across different repositories, with different digital identities and access rights. In many cases, user identities and access rights stay active for months or years after the job function changes or employment is terminated. Terminated employees with malicious intent could seriously damage HVA data and operations, particularly if they held privileged access roles prior to termination and those associated accounts remain active.

To improve the security posture of HVAs, identity and access management (IdAM) solutions with lifecycle management and automated approval workflow capabilities should be deployed to centrally manage the provisioning and de-provisioning of users consistently across all HVAs.

Using policy-based governance tools, an organization should correlate the different identities provisioned across the HVAs for each user, to uniquely identify every user and effectively manage and monitor who has access to what across all HVAs. For government agencies, the Homeland Security Presidential Directive (HSPD)-12 mandate has helped establish a unique identifier for each employee that could be leveraged to correlate the various identities provisioned to each user.

***PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.***

Besides proper management of identities and access rights, the other equally important part of access control is ensuring that access control policies defined for the resource are enforced when an entity attempts to access it. A common mistake or oversight in access control enforcement is to skip the authorization step following successful authentication of an entity, and thus have no restriction on the functions the entity can perform on the resource.

Authorization involves run-time decisions on what type of access the authenticated entity is allowed to the resource after the entity is successfully authenticated.

The organization must individually assess what type of access control to implement for each HVA. Common models for access control decisions are role-based access control (RBAC) and attribute-based access control (ABAC). Although ABAC provides more flexibility and finer grained control than RBAC, its suitability depends on availability of attributes from authoritative sources, clear definition and consensus among resource owners on the attributes used, and implementation of solutions to translate the access control policy into machine-enforceable rules. Guidance can be found in the *FICAM Roadmap and Implementation Guidance* document and in NIST SP 800-162, *Guide to ABAC Definition and Considerations.*

The access control's level of granularity depends on the data contained in the HVA. Compartmentalization may need to be enforced on the data to support various security needs, such as privacy or need-to-know requirements defined by the job function or the data consumers. For example, access controls may be needed to ensure that information in the entire database is not made available indiscriminately to all users authorized to access the resource. There might be a need to protect data at a row or column level and by type of user accessing the data. The right tools supported by well-defined business needs and access control policies are needed to effectively enforce access control to the resources. Access permissions to include roles or attributes should be governed and provisioned through the organization's identity lifecycle management (ILM) process.

Malicious actors, both inside and outside, will target accounts and credentials with administrative privileges, particularly those associated with HVAs. Additional best practices for privileged user accounts are listed below.

- implementing a standardized administrative process across all the HVAs
- taking stock of all the accounts provisioned and reducing their number
- implementing a tiered model for accounts with administrative privileges, with accounts in each tier restricted to administering a set of resources with similar risk level
- creating separate accounts with different credentials if the user has more than one role, to mitigate the risk of privilege escalation
- limiting assigned privileges to the minimum required for each role
- using dedicated workstations with no internet access for performing administrator functions, to restrict web browsing and email access to protect from malicious code and phishing attacks
- implementing solutions that offer just-in-time access with check-in and check-out account management. Accounts are provisioned temporarily and revoked after a pre-determined amount of time, with just enough privileges to perform the job functions on the resource.

***PR.AC-3: Remote access is managed.***

Remote access for HVAs should be disabled unless mission needs demand it. If remote access is needed, it should be limited to known users and services that have a specific need for remote access. Remote users, accounts, and credentials should be identified and managed to account for changes and updates in users or services requiring remote access. At a minimum, remote access policy for remote users and services should include the following information:

- level of access allowed for each remote user or service. Remote users with privileged access should have restricted access which may not allow full administrative access to network or system resources.
- devices that are allowed to remotely connect
- time periods when remote connections are allowed (e.g., 7 a.m. – 6 p.m.)
- time limit on idle connections
- IP ranges allowed
- remote connect tools and protocols allowed

- requirements for remote connections, including the type of encrypted connections and multifactor authentication

Access management systems should use the remote access policy to ensure that organizations manage which users or services are remotely accessing HVAs, from where, using which protocols, and performing which activities.

#### 3.5.2.2. Protective Technology

***PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.***

All creation and lifecycle management activities of identities, roles, and access rights should be logged, including the number of new identities created and new privileged accounts created. The logs should be reviewed and analyzed to ensure that the identities and access rights being provisioned are compliant with the access policies. Approvals, particularly for privileged roles, should be logged to ensure that there is accountability. Examining the logs will also help identify any abnormalities in user behavior, such as the following examples:

- unauthorized attempts to perform certain activities on the resources
- access occurring outside normal business hours
- access occurring from locations not expected for the job function
- privileged roles being provisioned that bypass the approval process
- excessive and frequent access to certain resources not normally expected for that job function or by the same digital identity

The different roles and the types of access associated with each role should be reviewed periodically and modified as needed. Reports generated by governance tools can reveal issues with the engineered roles, such as separation-of-duties violations and users accumulating excessive privileges, thus defeating the principle of least privilege.

Use of privileged accounts should be logged and the records reviewed to detect unusual activity. The NIST paper, *Best Practices for Privileged User PIV Authentication,* includes recommendations for automated reviews of privileged user access in accordance with law, regulation, and policy, and provides 30 days as an example frequency for the reviews.

#### 3.5.2.3. Awareness and Training

***PR.AT-1: All users are informed and trained.***

***PR.AT-2: Privileged users understand roles & responsibilities.***

All users should take cybersecurity training and remain aware of the threat landscape and their responsibilities for safeguarding their digital identities and credentials, and the data they access from the HVAs.

Privileged users, in particular, need to be fully aware of the impact on the organization if the accounts they use to administer the HVAs are compromised. They should be educated on the threats associated with the accounts and privileges they hold to perform their job. Each privileged job function or role should have not only customized security training on how to safeguard digital identities and credentials, but also technical training on the networks, systems, and/or applications they are responsible for administering.

Privileged users should be made aware of the consequences of creating workarounds for any HVA security controls and practices and misuse through role based awareness training. Privileged users with super privileges should be specially trained not to bypass approval processes or to assign privileged roles or escalate privileges to other users

at their own discretion. Acknowledgement and an agreement to the heightened roles and responsibilities should be recorded and tracked in accordance with ILM policies and procedures.

### 3.5.3. Detect

***DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.***

Analytic tools should be implemented to identify normal user and application patterns and behaviors to create a baseline profile for user or service access. This baseline profile is used to monitor and identify abnormalities in user and service behavior, such as the following examples:

- unauthorized attempts to perform certain activities on the resources
- access occurring outside normal business hours
- access occurring from locations not expected for the job function
- privileged roles being provisioned that bypass the approval process
- excessive and frequent access to certain resources by a digital identity that is not normally expected for the job functions assigned to that digital identity
- access by multiple digital identities occurring from the same host in a very short period

Reports generated using governance tools with analytic capabilities will help reveal defects, such as the following examples:

- users whose renewal of required training and certifications are past the stipulated renewal period
- roles with access rights that violate segregation of duties requirements
- users provisioned to access resources while their identity proofing or background investigations are incomplete or in need of renewal
- excessive number of users with privileged roles

### 3.5.4. Respond and Recover

***RS.CO-1: Personnel know their roles and order of operations when a response is needed.***

***RS.CO-2: Events are reported consistent with established criteria.***

***RS.AN-1: Notifications from detection systems are investigated.***

A fast and effective response when unauthorized access is detected relies on having a governance structure with well-defined business processes, so that appropriate authorities and IT personnel are rapidly engaged to evaluate and contain the attack by revoking access and preventing further damage to the assets.

If the governance reports reveal any gaps in full compliance with the access control policies, these gaps should be addressed promptly. For example, if a user is not up-to-date on required training, automated workflow tools could be used to temporarily disable the user's access, forcing the individual to complete the training; for remote connections, results from analytic or detection tools could prompt incident response teams to disrupt or terminate remote sessions.

It is good practice to periodically review access control policies and modify them to reflect the current threat, changes in the HVA's mission, new types of users (e.g., new partner organizations), and new regulatory requirements.

## 3.6. Authentication

One of the key actions stated in the CSIP is that all agencies will improve the IdAM of user accounts on federal information systems to drastically reduce vulnerabilities and successful intrusions.

Authentication is the process of establishing confidence in the claimed identity of an entity that is attempting to access a resource on a network. The credential presented during the authentication process is bound to the claimed identity. The types of credentials acceptable for authenticating to HVAs should include only those for which there is confidence in the vetting process of the entity's identity, and confidence that the entity presenting the credential is the one to whom the credential was issued.

Overall, strong authentication for HVAs involves the following actions, which are organized by CSF function:

- (Protect) establishing a governance structure. Developing well-defined business processes and policies for identity proofing and credential issuance. Implementing strong authentication using multifactor authentication mechanisms, eliminating the use of passwords.
- (Detect) monitoring to detect the presence of an attacker by looking for deviation from behavior normally seen or expected from the authorized user
- (Respond) putting in place procedures and points of contact to respond effectively if unauthorized access or use of stolen credentials is detected

### 3.6.1. Protect

***PR.AC-1: Identities and credentials are managed for authorized devices and users.***

Well-known user impersonation threats exploit the weaknesses associated with password-based single-factor authentication. Password vulnerabilities include guessing, dictionary attacks, social engineering, recovery from weakly encrypted password hashes, and use of key loggers. Strong authentication can be achieved with multifactor authentication that makes it difficult for the impersonator to supply the different factors required to gain access. The multiple factors include something in the user's possession, such as a hardware token, something known to the user, such as the Personal Identification Number (PIN), and some physical characteristic of the user (biometrics).

#### 3.6.1.1. Personal Identity Verification

Malicious actors target the accounts of privileged users, due to the privileges associated with their job functions as system administrators, network administrators, and database administrators. Therefore, strong authentication of users with privileged accounts for HVAs is critical.

The Cyber Security sprint initiated on June 12, 2015, has accelerated the issuance of PIV smart cards with X.509-based identity credentials for all users, and the PK-enablement of resources across the federal agencies. The CSIP directs agencies to transition to multifactor PIV-based authentication for all users, and the Cross-Agency Priority (CAP) goal is 100% for privileged users.

To facilitate agencies' PIV implementation, the General Services Administration (GSA) has established a Managed Service Offering to provide agencies with credentialing and identity services that comply with FIPS Pub 201-2. The agencies can also choose to operate their own card management systems and PKI to issue PIV cards to their employees. In either case, for successful lifecycle management of PIV cards, agencies need to ensure that they have reliable and secure connections between the authoritative sources for their users' identity data and the card issuance infrastructure. Exchange of information such as status of employee's identity vetting process, name

changes, and employment termination needs to occur between the credential issuance components and the authoritative sources for user data to issue, revoke, reissue or terminate the credentials in a timely manner.

Since the PIV credentials are based on X.509 digital certificates, the steps involved in the certificate-based authentication process include certificate revocation status checking and certificate path validation (*PKI-Auth* in Section 6.2 of NIST FIPS Pub 201-2). Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP) can be used to check the certificate revocation status. Since this is done in real time during the authentication process, HVAs need reliable network access to the OCSP responders and servers hosting the CRLs. Best practices are listed below.

- ensuring that the required ports and protocols to reach the revocation status services from HVAs are not blocked by firewalls
- employing caching mechanisms to disseminate the CRLs closer to HVAs
- deploying OCSP responders who are local to HVAs

Best practices for certificate-based authentication also include the use of strong cryptographic keys and hash algorithms. NIST SP 800-57 includes recommendations for key management. NIST recommends using Rivest–Shamir–Adleman (RSA) (2,048 bits), Elliptic Curve Digital Signature Algorithm (ECDSA) (curve P-256) keys, and Secure Hash Algorithm (SHA)-256 and SHA-384 hash algorithms.

Strong certificate-based authentication is effective only if the certificate presented during the authentication process is validated to the right certificate trust anchor. Operating system (OS) and software vendors, including web browsers, include a vast number of trust anchors in the certificate trust store for their products. Processes should be in place to identify the trust anchors needed for the HVAs to successfully authenticate users, including external partners. The certificate trust stores for each HVA should be managed and periodically reviewed to ensure that only the certificates of the appropriate issuing Certification Authorities (CAs) and the Root CAs are included to support the certificate path validation. Any unnecessary entries in the trust store should be removed.

Additional resources to assist organizations with PIV implementation are listed below.

- The GSA Federal Identity Credential and Access Management (FICAM) Program, in coordination with the Identity Credential and Access Management (ICAM) Subcommittee of the Federal Chief Information Officer (CIO) Council, guides federal agencies on how to implement various ICAM solutions at their organization. GSA hosts a repository using GitHub for the collaborative development of playbooks that includes a collection of technical guides and common code, scripts, and tools for agency implementers. The guides that focus on using PIV credentials for *logical access* such as authenticating to networks or applications, or digitally signing and encrypting, can be found at https://piv.idmanagement.gov/. The challenges, successes, and lessons learned from federal agency efforts to PIV-enable privileged account access have been collected and are being shared at MAX.gov, the Federal Community site for collaboration and information sharing.
- Phase 2 of the DHS CDM program includes services to help government agencies implement strong authentication to meet CSIP mandates and CAP goals. The Phase 2 services are based on the premise that the Microsoft Windows OS and Active Directory are the core components for enforcing network logon in an agency. As part of CDM Phase 2, the services offered to each participating agency include recommendations and scripts to facilitate implementing authentication to the agency's network, using PIV credentials if needed. The program also offers solutions to bridge non-Windows environments to Active Directory to enable PIV authentication for network logon.
- The NIST whitepaper, *Best Practices for Privileged User PIV Authentication*, discusses direct authentication with transport layer security (TLS) for relying parties (RPs) capable of supporting PIV authentication, and indirect authentication where the user authenticates to a verifier which then provides an assertion to the RP, since all HVAs may not be capable of direct authentication. The paper also discusses a transitional

proxy architecture where the proxy, placed between the privileged user and the target system, is PIV-enabled.

#### 3.6.1.2. Enhancements and Alternatives to PIV

##### 3.6.1.2.1. Enhancements to PIV

Based on threats observed by DHS, PIV may not be sufficient to manage the risk or potential impact of HVA compromise. The following options should be considered to augment current PIV implementations for HVAs:

- Contextual authentication uses a set of attributes to assess whether a user should be able to access a resource. Attributes include IP address, device type, geolocation of the access request, frequency of attempted access, or time of day. The attributes are determined up front and associated with a set of conditions that are used to develop policy rules for either providing access or requiring additional identity verification.

- Risk-based authentication uses attributes similar to contextual authentication, but results are combined into a risk score. The risk score is compared against a risk threshold to determine access. This mechanism is gaining popularity with financial institutions, where, for example, the authentication requirements are elevated if the user's activity goes beyond just viewing the account balance to transferring money from the account.

- Adaptive authentication dynamically adjusts the authentication methods required to access a resource. Any combination of authentication methods can be used as part of a step down or step up function; depending on the level of perceived risk, authentication mechanisms can either be made more or less stringent.

##### 3.6.1.2.2. Alternatives to PIV

Until systems transition to strong authentication using PIV credentials, other mechanisms to consider as a step up from single-factor password authentication are listed below.

- a two-factor authentication solution that uses hardware tokens generating one-time passwords (OTPs) at fixed intervals. The tamper-resistant tokens have a factory-encoded seed key and use a built-in clock to generate the OTPs. The authentication server associated with the resource being accessed matches the OTP the user provides with the expected code for the token in the user's possession. This authentication mechanism is widely used for establishing secure virtual private network(VPN) connections to the enterprise network. Many organizations are also using this method for privileged user authentication to provide stronger authentication than passwords.
- adoption of hardware-based security to support strong authentication (e.g., a Trusted Platform Module [TPM]). All major device vendors are embedding TPM technology in their products. TPMs are generally known for their use in checking system integrity during the boot process, but they can also be used for post-boot hardware-based security, and they can be used to protect the cryptographic keys associated with X.509 certificates. Some chip vendors also have developed technologies to generate OTPs in an embedded processor, eliminating the need to use a separate physical token.

#### 3.6.1.3. Privileged Access Management Solutions

Many vendors now offer Privileged Access Management (PAM) solutions to protect privileged user accounts by reducing the effectiveness of credential theft attacks such as the Pass-the-hash and Pass-the-ticket. PAM solutions should leverage PIV authentication services when possible to facilitate directory service and network access.

- One type of PAM solution uses a password vault that eliminates the need for privileged users to keep track of and use passwords to authenticate to different devices and systems to perform administrative functions. Privileged users authenticate to the vault using multifactor authentication; the vault then brokers sessions between the privileged user and the appropriate target device using a password. The privileged user does not have to know or maintain the password needed to access the target device. The vault also rotates passwords on the target devices at preconfigured intervals. Vault solutions can also support OTPs. Other PAM solutions include provisioning the privileged account temporarily for a predetermined amount of time, such as 8 hours, and with just enough privileges needed to perform the job function. This type of solution, which is also referred to as *just-in-time access*, requires integration with the organization's identity management implementation.
- Phase 2 of the DHS CDM program is offering agencies a password vault solution. Privileged users authenticate to the vault with their PIV credential. Vaults also offer session recording capabilities.
- Other gateway solutions provide the RP with an assertion of user authentication. The user (claimant) authenticates to a gateway solution with PIV credentials and the gateway provides the RP with an authentication assertion. NIST SP 800-63-3 defines *assertion* as: "A statement from a verifier to an RP that contains information about a subscriber. Assertions may also contain verified attributes." After successful authentication with the verifier, the claimant is issued an assertion or an assertion reference. The two types of assertions are *Holder-of-Key* and *Bearer.* For Holder-of-Key, the assertion contains a reference to a secret – a public or secret key in the claimant's possession that helps the claimant prove he or she is the rightful owner of the identity in the assertion. In the Bearer assertion, this capability does not exist and the RP must assume the presenter of the assertion is the one to whom the assertion was issued. Organizations should complete risk assessment tasks as described in NIST SP 800-63-3 to ensure that the appropriate gateway solutions are considered based on authenticator, identity and federated assurance levels.

With proxy or gateway approaches, care should be taken to ensure that they do not become the single point of failure. Password vaults used for privileged user access can be an attractive target to attackers, and a single compromise can give them access to several privileged accounts. Some factors to consider for password vaults are listed below.

- using a Hardware Security Module (HSM) to secure the solution's encryption keys
- architecting the solution to ensure continuity of operation
- assessing the risk associated with deploying the solution in a virtualized environment versus using dedicated hardware/appliance
- enforcing separation of duties and two-person control for privileged functions to protect against insider threat and compromised accounts

***PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.***

Issuance of credentials and all lifecycle management activities should be logged. Unsuccessful authentication attempts and the credential used should also be logged and appropriate alerts generated.

Use of privileged accounts should be logged and the records reviewed to detect unusual activity. NIST's paper, *Best Practices for Privileged User PIV Authentication,* includes recommendations for automated reviews of privileged user access in accordance with law, regulation and policy, and states 30 days as an example for the frequency of the review.

***PR.AT-1: All users are informed and trained.***

***PR.AT-2: Privileged users understand roles & responsibilities.***

***PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities).***

Users need to be instructed on how to safeguard their credentials and promptly report their loss. Privileged users especially need to be made aware of their responsibilities to ensure that HVAs are secure, and the extent of damage that can occur if their accounts are compromised. They should strictly comply with any organizational requirements to perform privileged user activities only on dedicated computing devices. Removal of the PIV cards when users step away from the computing device should also be standard practice.

If the HVA is linked with third-party stakeholders, then it is imperative that they also have similar training and awareness to prevent them from being the weakest link that malicious actors can exploit to gain backdoor access to the HVA.

### 3.6.2. Detect

***DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.***

Continuous monitoring of access to HVAs may not necessarily identify a stolen credential, since the attacker will be masquerading as the authorized user. However, monitoring should help identify deviation from behavior normally seen or expected from the authorized user, for example, number of resources being accessed, time/place of access, frequency of access, or attempts to escalate privileges.

The NIST paper, *Best Practices for Privileged User PIV Authentication,* includes recommendations to automate monitoring of all privileged access; it also emphasizes that monitoring is particularly important for legacy systems that do not support PIV authentication for privileged access at the appropriate level of assurance.

### 3.6.3. Respond

***RS.CO-1: Personnel know their roles and order of operations when a response is needed.***

***RS.CO-2: Events are reported consistent with established criteria.***

***RS.AN-1: Notifications from detection systems are investigated.***

If unauthorized access or use of stolen credentials is detected, procedures, points of contact, and communication channels need to be in place to respond effectively. For example, credentials may need to be revoked immediately or access control policies may need to be changed. Personnel with the right roles and authority need to be promptly notified to take appropriate actions.

A response strategy should be in place to analyze intruder behavior and the scope of the attack. For example, just revoking or reissuing stolen credentials may not be sufficient if the attacker was successful in installing malware or rootkits that could be used to regain access. After each event involving access with a stolen credential, the response plan should be revisited and updated to incorporate the lessons learned from the attack.

## 3.7. Network Segmentation

There was a time when physical *air gap* segmentation was the only choice for securely isolating networks from each other. However, the spread of virtualization (including VPNs) has brought with it new ways to implement network segmentation. Enterprise networks may combine *physical*, *logical*, and *virtualized* segmentation techniques that vary by network type.

Segmentation should be done at all layers of the Open System Interconnection (OSI) protocol stack. The goal is to isolate, to the maximum extent possible, entities at a given layer from each other, on the theory that segmenting within each layer will help protect the other layers. Any connections between processes and data in one layer with those in another must be through controlled interfaces.

The following subsections outline best practices for HVA network segmentation and, if applicable, reference CSF aspects (categories and subcategories) that apply specifically to network segmentation. Overall, network segmentation for HVAs involves the following actions, which are organized by CSF function:

- (Identify) identifying entities accessing the HVA, their operational behaviors, interactions, and inbound and outbound data flows to create and prioritize segmentation rules and policies
- (Protect) segmenting data flows and providing boundary protection. Depending on the organization's maturity, techniques could include virtual local area networks, Layer 3 filtering to restrict access, Network Access Control (NAC), IDS / Intrusion Prevention System (IPS), or a zero-trust network with software-defined networking (SDN) and network function virtualization (NFV).

### 3.7.1. Identify

***ID.AM-3: Organizational communication and data flows are mapped.***

***ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.***

#### 3.7.1.1. Network Identities

Good practice requires identifying the entities (and their roles in) accessing the HVA, and noting their operational behaviors and interactions with the HVA. It also requires identifying inbound and outbound HVA data flows. This information is needed to create and prioritize segmentation rules and policies for which entities and flows access the HVA segment, and which flows are to be allowed to leave the HVA segment.

Network segmentation is based on one or more identities associated with a *protocol data unit* (PDU). Every PDU is composed of a block of layer-specific information (its header) and a payload, laid out in a hierarchy as illustrated in

*Figure 2*.

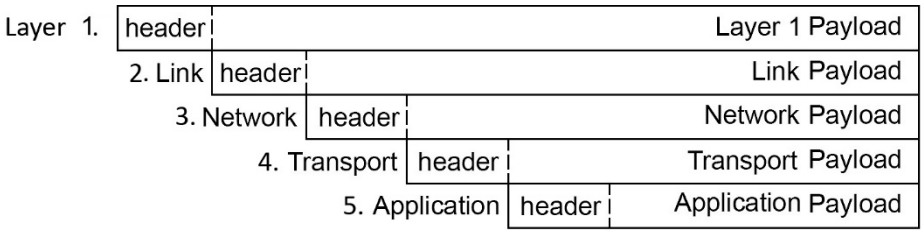



*Figure 2. Network Segmentation Hierarchy*

In most cases, segmentation is first applied at the network layer, but, for an HVA, segmentation must also be applied to multiple layers to be effective. Example applications are provided below.

Segmenting based on data link layer identity. If all user endpoints potentially having access to the HVA are on a single Local Area Network (LAN) (e.g., a single IEEE 802.3 segment) attached to an HVA entry point (e.g., an IP router or a link layer switch), then endpoint identities in most cases can be reliably determined by data link layer identification contained in link layer frames, such as IEEE standard 48-bit Media Access Control (MAC) addresses. It is then possible to segment the external LAN from the HVA LAN by blocking unauthorized or unknown MAC addresses at the boundary.

Segmenting based on network layer identity. All but the very simplest home office network routers are capable of segmenting attached networks by network layer information, such as 32-bit Internet Protocol version 4 addresses (IPv4) or 128-bit IP version 6 addresses (IPv6). The most common and most efficient way to enforce IP address-based segmentation is to initially filter network traffic by IP subnetwork addresses, and then to filter by endpoint addresses, possibly in combination with higher level information (e.g., transport layer information). Some caveats apply to using network layer addresses as identities:

- Statically defined IP address filtering may be rendered ineffective by the Dynamic Host Configuration Protocol (DHCP). DHCP is widely used for assigning IP addresses and other configuration data to endpoints when they bootstrap. Many DHCP implementations periodically update endpoint devices after bootstrap.
- Binding between a network layer address and a MAC address is not mandatory. In general, other than in virtual machines (a staple of cloud computing), MAC addresses are permanently embedded in hardware by network interface manufacturers, while network layer addresses are assigned and reassigned to devices as needed by system or network administrators, or by a DHCP service.

Segmenting based on transport layer identity. Many network routers are capable of filtering network traffic using a combination of transport-layer and network-layer information. In the Transport Control Protocol (TCP)/IP protocol suite, standardized network services are identified by assigned port identifiers in the transport-layer header. This makes it possible to segment networks with reasonably fine granularity by examining source and destination network addresses in combination with the service identified by the destination port number if it designates a standard service such as email delivery. Some caveats apply:

- It is easy for an endpoint to spoof the binding between a port number and a service. For example, the standard port number 25 is assigned to the Simple Mail Transport Protocol (SMTP) service, which uses TCP as its transport layer. It is possible to implement an SMTP service that uses a non-standard port, a non-standard transport layer, or both.
- It is easy to implement a service other than, for example, SMTP that accepts incoming TCP network traffic on Port 25.

With these caveats in mind, for strong assurance that the network service implied by a transport-layer port identifier is accurate, it is necessary to either inspect network traffic content and compare it to the application layer protocol, or attempt to make a client connection to the putative service. This topic is explored further in Section 3.7.2.1.2. In many cases, implementing a *proxy* application service at the organizational network boundary is a highly effective way of selectively isolating the organizational network from external networks. World Wide Web proxies are widely used, for example.

Segmenting based on application layer identity. In the general case, it is not possible to segment a network at the network boundary using application-level identifiers alone because they are all internal to instances of specific applications (e.g., email, World Wide Web, file transfer). To segment an organizational network at the application layer, application proxies are required, and, to ensure that the proxies are not easily bypassed, boundary enforcement of network- and transport-layer segmentation is also required.

### 3.7.2. Protect

***PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.***

#### 3.7.2.1. Segment Data Flows

Network data flows to and from an HVA, and the flows within it, must be isolated from other flows. A common way of doing this is by encrypting flows at one or more layers of the protocol stack. If encryption is applied to the IP layer, the result is a VPN that tunnels transport layer segments (i.e., TCP) or datagrams (User Datagram Protocol [UDP]). Another way to isolate flows, albeit not secure, is to use virtual LANs (VLANs).

When encryption is used to protect a flow, the encryption must have appropriate strength (a measurable result of combining a key length with an encryption algorithm), for the flow. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* provides examples of data flow restrictions:

- blocking outside application- or network-layer traffic claiming to be from within the organization (e.g., inbound email claiming to originate from an internal email address)
- blocking web requests to external websites that are not from the HVA's web proxy server
- restricting information transfers between the HVA and external organizations based on analysis of data structures and content

Some organizations enforce "Deny-All, Permit-by-Exception" (DAPE) policies for HVAs that do not support any applications or traffic inflows/outflows other than those that are absolutely required; even then, their implementation does not directly expose internal HVA functions to external entities. For example, if an HVA absolutely *must* support SMTP email delivery, then the HVA must either include an email proxy or have access to an organizational (presumably dedicated) email proxy. In either case, only HVA-authorized users would have access to the SMTP service. Such an email proxy service would also be required to implement suitable content screening to prevent information leaks and block incoming malware or unsuitable content.

##### 3.7.2.1.1. Segment Stored Data

Co-locating large volumes of data in a single HVA system offers so-called one-stop shopping for a successful attacker. Storing different types or classes of data on different HVAs, and then maintaining only partial data sets of each type or class, makes an attacker's task considerably more difficult, albeit at the cost of making implementation and maintenance costlier and somewhat more complex.

##### 3.7.2.1.2. Enforce Protocol Formats

Disguising illicit data in network traffic is easily done by inserting a well-known port value in a transport-layer header. For example, the presence of Port 25 as either the source or destination application in a TCP payload *implies* that the payload's application is the SMTP protocol, which has well-defined format rules for the envelope it creates for user application data (e.g., all elements of the standard SMTP envelope are ASCII [American Standard Code for Information Interchange] text). Whether the TCP payload is actually SMTP can be determined to some extent by examining the envelope. If the SMTP envelope is malformed, it *could* be disguising illicit data.

Format enforcement must be applied bidirectionally to detect both attacks against services and attempts to exfiltrate data. Enforcement must also be informed by known facts about the HVA's infrastructure. For example, if traffic is being sent to or from a putative SMTP server, then the IP address of the server endpoint must obviously be that of the HVA's SMTP server.

Note that it is impossible to enforce protocol formats while data is in transit if the link, network, or transport-layer payloads are encrypted. In general, the protocol format enforcement function must reside on endpoints, perhaps as a component of a host intrusion prevention system (HIPS) or an on-host firewall.

#### 3.7.2.1.3. Segment Network Flows by Their Function

Certain types of network traffic, such as security, device (e.g., Storage Area Network [SAN], Network-Attached Storage [NAS]), and network management/control traffic, *must* be isolated from production flows and from each other. The methods for achieving isolation will vary, but physical isolation from the production network should be considered first because of the severe impact of a successful attack against such traffic. Even with physical isolation, encrypting individual or application-specific traffic flows may be appropriate.

Where feasible, the range and types of operations supported by management/control function interfaces should be minimized. In some cases, this might mean requiring physical access to affected equipment to perform certain privileged operations, but in no case should all possible operations be allowed by all endpoints.

#### 3.7.2.1.4. Implement Host-Based Protection – Firewalls, HIPS, and Whitelisting

In a multi-host HVA, individual hosts need to be shielded from each other to prevent lateral attacks, where an attacker exploits a weakness in one host and then uses that host as a trampoline for attacking others. In this protection scheme, each host is configured to only allow incoming network connections from a subset of other HVA hosts, and only for specific protocols. For example, Host A might accept only SMTP connections (but no other application protocols) from Hosts B and C (but from no other hosts). A typical host-based protection implementation would have one or more components: a firewall, a host intrusion detection system (HIDS), and a HIPS. In most cases, a configuration that applies whitelisting rules would be simplest.

#### 3.7.2.1.5. Using Mandatory Access Controls to Protect Host Processes and Data

Discretionary access controls are host-specific access controls that can be changed at will by a privileged user identity (e.g., *administrator* for Windows, or *root* for Linux systems). In contrast, mandatory access controls cannot be changed without rebooting the system after changing its security-relevant configuration. Mandatory access controls eliminate the need for a privileged system user identity with unrestricted capabilities by making it possible to assign different capabilities to different user identities. There are several ways of describing mandatory access controls, although the most familiar example is based on a strict hierarchy of formal data classifications/compartments/user clearances (e.g., *UNCLASSIFIED, SECRET, TOP SECRET, SENSITIVE COMPARTMENTED INFORMATION [SCI]*), combined with an implementation possessing the Bell-LaPadula property. Considerably more sophisticated, albeit more complex, mandatory access control implementations also exist.

Mandatory Access Controls partition a computer's devices, data, processes, and users into multiple groups, and defines immutable internal access controls governing the interactions between groups. For example, Mandatory Access Controls would provide a solid foundation for the host-based protection described above.

#### 3.7.2.1.6. Virtual Private Networks

Network segmentation can be enforced by using encryption to isolate flows from each other; encryption is also used to create VPNs. Assuming initial VPN access is controlled by PIV or other two-factor mechanism and is protected by suitable encryption, a VPN can be used to isolate either individual or groups of client/server flows. General-purpose VPNs are usually created in the network layer (Layer 3) using IP Security, which encrypts the entire network-layer payload of transport and application data.

Transport-layer (Layer 4) VPNs are also common, for example to isolate individual web sessions using either TLS or Secure Sockets Layer. If used alone, transport-layer encryption leaves the network layer information exposed but encrypts both the transport and application layers.

#### 3.7.2.1.7. Layer 2 Virtual LANs

A single LAN can be expanded to include other LANs on an organization's internetwork, thereby creating a VLAN with multiple segments. Conceptually, a VLAN is a single Layer 2 broadcast domain composed using multiple collision domains (i.e., LANs). On legacy organizational internetworks, VLANs are typically stitched together using one or more Layer 3 routers that also implement Layer 2 switching. More recent VLAN implementations may include support for OpenFlow and SDN, and VLANs may be defined using information from OSI layers up to and including Layer 7 (application).

VLANs are not by themselves a secure segmentation choice, so VPNs should be used to isolate VLAN flows from each other.

#### 3.7.2.1.8. Using Layer 1 Segmentation to Isolate an HVA

The most secure way to isolate network flows from each other is to use dedicated physical links (preferably fiber optic) between endpoints. Separate hardware links would still be appropriate for handling network flows that have very different security requirements: for example, network management devices often require console and operations (command and control) interfaces that are isolated from the networks under management.

Physical isolation might be justifiable for HVAs that store and process sensitive but unclassified information that is accessible only to small numbers of authorized users. While physical isolation guarantees a segmentation boundary, it requires replicating many, if not all, infrastructure services within the HVA, which requires hardware and software replication, maintenance that adds to costs, and operational barriers (e.g., it becomes necessary to manually carry all data into the HVA area and load it into HVA storage, followed by an inverse process for exporting data from the HVA). Because of these issues, organizations may want to consider the techniques used in a cross-domain solution before resorting to physical HVA isolation. Furthermore, physical segmentation is not absolute, as there will likely need to be flows into the environment on removable media to provide patches and updates, which must be carefully controlled.

#### 3.7.2.1.9. HVA Boundary Protection

An HVA will in general require network boundary protection that honors organizational boundary protection and enhances protection through configuration. Examples are listed below.

- one or more network firewalls. These would protect against attacks on the HVA at the link, network, transport, and application layers. Protection functions against external attack might be implemented serially on separate devices for isolation or to simplify maintenance, or redundantly for robustness. An example of defense at the application layer for email would be analysis of attachments for evidence of malware, verification of external source domains, and verification of internal sources.
- one or more standards-compliant credential services (e.g., X.509-based PKI) with access to external peer services when necessary for PKI and authentication
- one or more application proxy servers dedicated to HVA support. These would deliver protection for basic user applications such as web, email, and data movement, and if called for, would assist in cross-domain solutions, high-speed link access, and high-volume encryption/decryption (e.g., HSM). The proxy servers should include, as needed, support for secure remote HVA user login, session management, data movement, and display. In some cases, specific applications may need proxy servers for user access within the HVA.

- a uniform but flexible form of business integration and data transfer, such as Enterprise Service Bus (ESB) or data drop boxes
- internetwork routing that includes bidirectional IP address-based access control and possibly network address translation (NAT)

#### 3.7.2.2. Segmentation and Zero Trust

A US House of Representatives Committee on Oversight and Government Reform report recommends that agencies adopt the zero-trust model of cybersecurity.[xxx] *Zero trust* in the context of network segmentation involves a layered security model where computers residing in an enclave (e.g., users) are given only restricted access to other enclaves (e.g., applications). Implementing zero trust should require the following items:

- asymmetric access controls and controls based on associations between certain computers and certain applications, putting logical perimeters around data or assets so that granular rules can be enforced
- measures to visualize, inspect, and log all HVA network traffic for both malicious activity and areas of policy improvement
- HVA boundary protections replicated internally in the HVA at the host level and even at the user application level. This partitions the HVA itself into segments consisting of one or more hosts for each application, and partitions each host along the lines of local application boundaries.

An overview of zero trust networking written by Forrester Research for NIST in 2013, *Developing a Framework to Improve Critical Infrastructure Cybersecurity,* provides additional guidance on implementing a zero-trust model.

##### 3.7.2.2.1. A Sample Segmentation Use Case: Email Support for an HVA

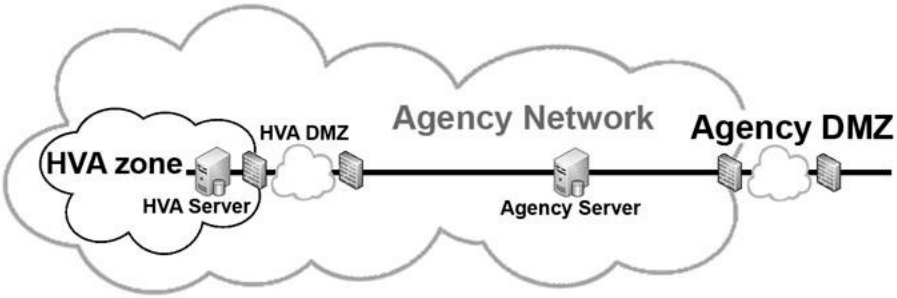



*Figure 3. Example Multi-level Segmentation*

A highly simplified example of multilevel segmentation using an email delivery service illustrates segmenting an application suite along the lines of its layers *and* segmenting Layers 2–4 connectivity. Figure 3 illustrates one possible way to implement an organizational email delivery system. As shown, the agency network has an external demilitarized zone (DMZ) network, bounded by a pair of firewalls. Basic services, including NAT and proxy, necessary for external communication are in the DMZ, as are certain agency-wide security services. An agency-wide SMTP server is located on the agency network behind the agency DMZ network; it forwards email to endpoints and other servers within the network, including an email server dedicated to HVA use, located behind the HVA's DMZ network.

The system design should include the following features:

- The email service (if any) on each host within an HVA boundary must not accept direct incoming connections from hosts that are not within the HVA.

- Internal HVA hosts must not be allowed to establish direct Layer 4 connections to external email hosts or services.
- The HVA email service must not accept email for delivery to any user or host identity that does not exist within the HVA boundary, or to one that has been deemed ineligible for email delivery.
- Most user identities in this category would be privileged pseudo-users such as *root* or *administrator.* These are anonymous user identities, and, with few exceptions, such users must not be allowed to send email to remote hosts, whether or not the remote hosts are within the HVA boundary.
- The HVA email service must not accept any messages from unrecognized domains or from domains known to harbor malicious or inappropriate activity. Similarly, it must not allow messages to be sent from the HVA to unknown domains, or to domains that have an invalid or missing DNS MX (Mail Exchange) resource record.
- The email service should check all incoming messages for malicious content or explicit internal references (e.g., URLs) to known attack domains and refuse to deliver such messages to end users, including checking email header information for consistency.
- Every host within an HVA must, if appropriate and feasible, have local malicious content protection for every local application.
- Every local email client on each HVA host must be using the most recent production version of its software, including the most recent production versions of any applications the client uses (e.g., for displaying images or word-processing documents).

#### 3.7.2.3. HVA Evolution: Virtualized Computing

A highly simplified illustration of virtualized computing is shown in Figure 4. All virtualization has three layers:

- a physical platform, which includes a physical CPU, stable and volatile storage (high-speed memory and secondary storage), TPM, clock, etc.
- a Virtualization Layer, consisting of a Virtual Machine Monitor (VMM) and any associated modules (e.g., virtualized device interfaces, security modules)
- a Virtualized Context that is provided to Virtual Machines (VMs). What is exposed (e.g., as a device application programming interface [API]) to a VM depends on its type and requirements.

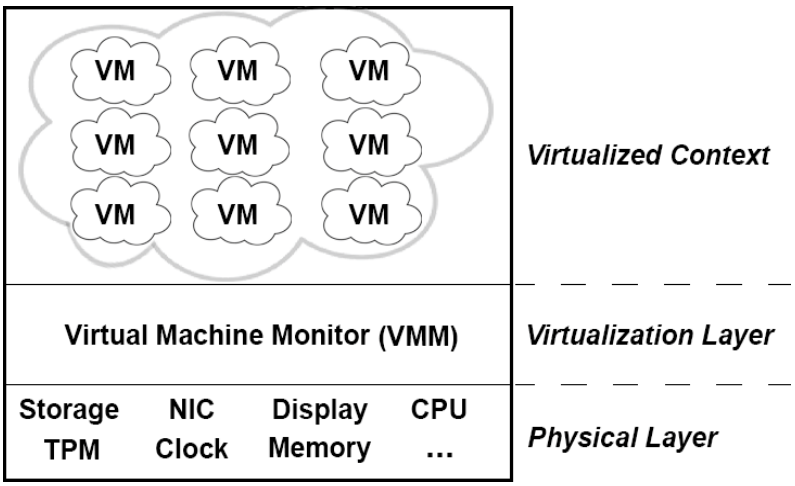



*Figure 4. Virtualized Computing Simplified*

The Virtualized Context includes one or more VM instances. Provisioning for these (e.g., memory, stable storage, network address, CPU) depends on VM subscriber option choices.

In the context of cloud computing, segmentation – along with nearly everything else in existing computing centers, including the virtual computers and devices that are exposed to users – will be virtualized, which means segmentation and the networks or applications it is applied to will be implemented almost entirely in software. All foundational networks in computing centers will soon be switch-based (i.e., Layer 2) and controlled by SDN, with control functions implemented as NFV.

SDN is the centerpiece of the software-defined data center because it implements both the governing rules and implementation mechanisms behind segmentation. It can also enable what has been called *network micro-segmentation.* With micro-segmentation, HVA owners could create highly customized equivalents to firewalls: for example, assets might be given a uniquely configured firewall using a combination of conventional rules and flow definitions that could be equivalent to VLANs, all backed by ABAC terms (e.g., time-of-day or geographic rules). Each virtual firewall on the network can be dynamically reconfigured to respond to events, such as an attack in progress sensed by a (virtualized) IDS.

NIST SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection,* describes segmentation configurations for VM protection in cloud computing. Best practices are provided for the following segmentation configurations:

- isolating VM processes from each other
- virtual switches (Layer 2)
- virtual routers (Layer 3)
- virtual firewalls (primarily Layers 3 and 4, but often including Layers 5–7 as well)
- implementing VLANs (Layer 2)
- overlay-based virtual networking

#### 3.7.2.4. Implementing Segmentation: An Evolutionary Approach

Implementing network segmentation is an evolutionary process. The process described in this section focuses on technical issues, although the human factors affecting security are noted. It is neither an exhaustive nor normative treatment of the topic: for example, organizations will have different security needs, organizational structures, and workflows.

The weakest links in organizational network security are well-intentioned employees, not computing systems or networks. Social engineering, primarily in the form of email phishing, is the dominant attack vector for gaining initial entry to organizational networks, and it is likely to remain so for the foreseeable future. The high success rate of phishing attacks is an excellent example of why a defense that uses multilayer network segmentation – including the so-called *human layer* of the protocol stack – is important.
The early stages in network analysis and defense implementation lay the foundation for everything that follows. One school of thought asserts that the best analytic procedure views the network as a target in the same way that attackers eventually will. The broad flow of the analysis is to start with an examination of the network topology, its purpose and users, and conclude with a strategy (and tactics) to detect stealthy attacks and defend the network.

##### 3.7.2.4.1. Know the Network Better Than Any Attacker

Attackers usually begin by examining the purpose and structure of an organization's network(s). As a rule, this will be a minimum-profile activity that follows an initial penetration and persists for weeks or months. Accordingly, an organization's first task is to know its network and assets.

- Accurately determine the current topology and state of the network. Initially, this is required to establish baselines that can be used later to detect changes. Note that most of the information obtained at this stage is sensitive because of its potential value to attackers.

- Establish one or more pilot network operations centers (NOCs) and network security operations centers (NSOCs) using commercially supported and standards-based (e.g., based on Simple Network Management Protocol [SNMP], Microsoft Network Monitor [NetMon]) network management packages. Initially, NOCs and NSOCs may consist of a very small number of computers and operators. In a geographically distributed organization, hierarchical NOCs and NSOCs are worth considering. An important prerequisite for this stage of evolution is to determine which management protocols are supported, and by which devices.
- Map the network topology and its cut points, including all network backbones, internal branch office internetworks (including LANs, VLANs, Multi-Area Network, and Wide Area Network [WANs]), and connections to external networks (e.g., to regional internet service providers, peer organizations, contractors).
- If the discovered network topology is a flat network (i.e., an organization-wide switched [Layer 2] as opposed to routed [Layer 3] network fabric), begin designing and instantiating a hierarchical architecture (an internetwork, i.e., a network of networks) where multilayer segmentation can be implemented from the physical layer up. An important goal of this activity is to uncover traffic cut points and choke points in the network that could hinder incident response operations. These are also valuable as vantage points for attackers passively monitoring the network as part of their survey operations.
- For every IP subnetwork, LAN, and VLAN discovered during the mapping topology described above, obtain device/user admission policies, if any. This information may be used later to establish portable, organization-wide and standards-based device/user network admission policies.
- To the extent possible, monitor each subnetwork, LAN, and VLAN to determine their actual uses, traffic volume/application patterns, etc. Traffic monitoring will become a permanent activity that evolves from the initial set of samples to random sampling done to detect usage shifts or possible intrusions. A legal mandate for monitoring will usually involve notifying end users and system administrators about the activity.
- Identify and locate all HVAs attached to the network. What counts as HVA data will differ according to its use, but some cases are obvious: systems containing Personally Identifiable Information (PII), medical records, controlled unclassified information data, formally classified data, financial data.

o Perform initial, and then recurring, organization-wide technical vulnerability assessments and failure analysis based on assessment results.
  - The purpose of technical vulnerability testing is to expose physical, protocol, procedural, personnel, and software risks. This activity is not the same as penetration testing, where the goal is to defeat security protections by exploiting vulnerabilities.
  - As with traffic monitoring, technical vulnerability assessments must recur at unpredictable intervals to be effective. Unlike formal accreditations, technical vulnerability assessments are generally ad hoc and make extensive use of the same tools that attackers might use to map networks and expose potentially exploitable weaknesses.
  - A vitally important component of vulnerability assessment is *failure analysis*. Not every vulnerability directly results in a serious security exposure, but in large, complex systems (and even some small, simple ones), a weakness in one component may lead to catastrophic failures at the terminus of an avalanche of minor failures. Vulnerability assessment is the first step in a larger analytic process that supports implementation, and eventually SIEM (see below).
  - Note that vulnerability assessment and failure analysis may expose unexpected HVAs.

o Establish baseline HVA policies and mandates using the results of topology, state, and vulnerability assessments.
  - Initial baseline policies must *all* be achievable by *all* affected branches and offices in a short time (e.g., a few weeks). An initial goal is to fully comply with the FISMA requirement to "implement policies and procedures to cost effectively reduce risk to an acceptable level." Longer deadlines can

be set for resolving lesser shortcomings. Due to budget constraints, however, resolving more costly or complex shortcomings may also require longer deadlines.

- HVA operators should model and test segmentation policies before deploying them operationally. Organizations should consider testing that includes using alarm triggers designed to help understand business disruptions a policy might create and adjust the policy accordingly before deployment.

#### 3.7.2.4.2. Determine HVA User Communities and Eliminate All Unnecessary/Unprotected Services within the HVA

- Using data obtained from 1 (above), determine HVA user communities and eliminate all unnecessary or unprotected services within the HVA – and begin to implement a fully standards-compliant PKI that controls access to the remainder.
- Each HVA should have a clearly identified user community and associated application-specific network traffic flows. Note that many HVA users may be daemon programs executing on authorized remote servers and acting on behalf of authorized remote users, possibly in external organizations. To the extent possible, control all external access to HVAs using a combination of VLANs and VPNs or, if called for, unequivocal evidence of physical user presence. Daemon processes supporting user applications should enforce two-factor user identification (e.g., PIV) and validate end-user identities to HVA processes.
- A different approach would be to implement an HVA-specific PKI and make HVA-specific user communities the initial user groups. Experience gained since approximately 2000 implies that implementing a PKI can be a challenge, but the rewards outweigh the start-up costs.

#### 3.7.2.4.3. Design and Implement a Fully Segmented (or Zone) Architecture that Includes a PKI

- Network segmentation is used for reasons that go beyond security considerations; the general idea is to end up with a robust and secure network architecture, with an internetwork (i.e., network of networks) being the proven model.
- A segmented (also called *zoned*) network containing HVAs will generally be designed using an architecture like the one illustrated in Section 3.7.2.2.1, where HVA access is controlled using the same basic DMZ architecture as the one used to protect the organization's network. If possible, the information gathered in 1 (above) might be used to segment users and applications attached to HVAs to prevent information leaks.

#### 3.7.2.4.3. Implement a Security Information and Event Management System

- A SIEM system allows system and network managers to determine whether disparate activities or anomalies are related, including whether they are security-relevant. A successful SIEM implementation depends heavily on implementing the three steps described above and having in place sustained operations such as traffic and topology monitoring that can be used to detect anomalies and successfully halt attacks. In nearly all cases, SIEM depends heavily on an ability to communicate with diverse organizations to share timely information about recent or ongoing attacks – and, inevitably, failures.

# 4. LEVERAGING COMMERCIAL CAPABILITIES

Careful consideration and selection of technology and automation solutions can significantly improve an organization's ability to manage IT resources and use IT staff effectively. Taking time to identify specific challenges and gaps in existing capabilities allows organizations to better articulate requirements and choose the right tools.

Organizations should consider which tasks can and should be automated. Repetitive, consistent, and time-consuming tasks may be good targets. Searching audit files to identify specific patterns (e.g., error codes, attack

signatures) represents a task well-suited for automation. Conversely, automation may not be appropriate for tasks that require contextual or qualitative analysis and decision making.

Budget is another significant consideration when comparing potential tools and solution sets, and several factors should be evaluated. Initial costs can include product evaluation/pilot, product licensing, hardware investments, engineering and implementation in the target environment, and training. Sustainment costs can include software and hardware maintenance/support fees, upgrade costs, and training (for new personnel and product changes). Complexity of the solution and the environment in which it operates can also impact costs over the solution's life cycle. Organizations may need to compare inexpensive tools that require highly skilled or specialized administrators against tools that come with high initial implementation costs but low long-term maintenance costs. Some vendors offer product suites with a wide range of security and network management tools and centralized management solutions, which may be an ideal choice for organizations where integrating security technologies into a single management solution is a significant factor.

Choosing the right tools requires knowledge of the organization's specific objectives and constraints. The following subsections provide guidance for selecting commercial tools to address patch management, malware defense and anti-phishing, access controls, authentication, network hygiene, and network segmentation.

## 4.1. Patch Management

Patch management can be a complex challenge, especially in large organizations with diverse endpoints. Tools in this capability area vary widely in terms of cost, complexity, and integration with other tools or solutions, so having clear requirements is crucial.

The first thing organizations should consider is the type and diversity of endpoints to be managed. Some tools are designed to address specific platforms (e.g., Windows, Linux). Others support multiple platforms and third-party software. Tools that offer support for multiple platforms are likely to be more complex and more expensive to maintain compared with tools for specific platforms. More complex solutions, however, may be ideal if they offer solutions for other challenges. Vendors often package patch management tools in suites, with products designed to address a variety of management and security functions.

Organizations also need to consider the tools and solutions they already use (e.g., asset/inventory management, vulnerability identification/scanning, configuration management, patch deployment, auto-update). Some patch management tool(s) can be integrated with other endpoint and/or network management solutions, so integration may need to be acknowledged as a potential requirement.

Finally, organizations should consider which patch management activities are good targets for automation (e.g., checking availability of new patches, downloading patches/updates, and scheduling distribution and installation). They may also need to consider if all endpoints within the environment should be targeted equally for automated activities. Considerations in weighing the benefits and risks of automation should include the average failure rate of automated patching activities (resulting in the need for manual intervention); the projected window of exposure (i.e., increase or decrease in exposure based on the automation decision); and whether automating patch management activities creates additional time for other critical activities.

## 4.2. Malware Defense and Anti-Phishing

To defend against malware and phishing attacks, organizations should apply the defense-in-depth principle. Layers of protection can be achieved by using protection and detection capabilities at gateways and endpoints. Automation to keep tools current is essential to overall effectiveness, and commercial vendors in this space generally offer tools that cover many aspects of malware and phishing defense, with centralized management and

automation options. When considering solutions, organizations may want to pick a vendor that can provide solutions at multiple layers and for multiple platforms to reduce complexity, although it can be advantageous to use different tools/vendors at different layers/platforms within the organization's architecture to maximize protections. In addition to technical safeguards, user education/training remains a key factor in reducing successful malware and phishing attacks. This section discusses gateways and endpoint tools, as well as application whitelisting.

Organizations should use ingress and egress filtering at boundary entry and exit points (e.g., email and web gateways). Anti-malware software is widely available for integration with mail transfer agents at the email gateway for detection of malware and phishing attacks, spam, and other undesirable or restricted content. Many vendors in this trade space offer products that integrate anti-malware detection with web gateway technologies. These tools prevent introduction of known malware using a variety of techniques, including signature-based detection and blacklists of known malware sources. Suspected malware can be prevented using heuristic-based detection of malware-like behavior or patterns. Undesirable content (e.g., executable attachments and active content) can be reduced via application hardening and customized filtering policies/rules. Additionally, many of these vendors offer data loss prevention capabilities to detect and prevent data breaches and data exfiltration.

Endpoints must also be protected from malware. Operating system malware prevention technologies can help mitigate common techniques used in the exploitation of vulnerabilities. Traditional anti-virus/anti-malware software for endpoints is another key component in an organization's malware prevention strategy. A wide variety of vendors have endpoint malware prevention and detection solutions that offer server/workstation applications and centralized management. Automated signature updating is necessary to keep these tools current. Updates can be distributed from an organization-controlled centralized system or directly from the vendor.

Application whitelisting tools can prevent execution of any application that has not been specifically authorized for use. Developing a comprehensive whitelist on user workstations can be challenging, because users often perform a wide variety of activities, and the rate of change may be high. Developing a whitelist for a server is generally much easier, as server functions tend to be highly consistent and repetitive (especially when best practices have been applied to minimize services and features on the system). Many vendors that offer traditional and gateway anti-malware products also offer application whitelisting tools that integrate into their centralized management solutions.

## 4.3. Access Controls

Access controls must be applied throughout the HVA. Port-based network access controls (e.g., IEEE 802.1X certificate-based authentication standards, static or dynamic media access control configuration,) and other NAC solutions provide assurance that only authorized systems can connect to and communicate on a defined network or segment.

IdAM solutions can be leveraged to authenticate people and non-person entities (NPEs), as well as authorize access to information, services, and resources. People and NPEs can be organized into groups to which security policies are applied. Policies need to be based on the least privilege principle, such that only activities required to perform job duties are authorized. For example, the ability to alter system configurations and install or remove software should be limited to trained administrators with designated responsibilities for these activities. Organizations can reduce threats to HVAs from internal and external entities and achieve more granular access accountability for monitoring and auditing activities through consistent security policy enforcement.

Application proxies can be used to broker inbound communications with HVAs. For example, a web application firewall can be used to protect web applications (including web services) from malicious requests, such as Structured Query Language injection or cross-site-scripting attacks. These tools can be deployed in monitoring mode to learn typical application behavior and automate the development of security policies based on that

behavior. Non-routine application functions need to be exercised during the learning process to ensure that the resulting security policies allow less frequent authorized application activities. Then, the tool can operate in enforcement mode with greater assurance that legitimate application functions will operate as expected.

Encrypting data in transit, in process, and at rest helps to protect the confidentiality of sensitive HVA data and prevents unauthorized access. Organizations should carefully consider which data elements and transactions need to be protected with encryption. Using encryption can affect monitoring capabilities, so the costs and benefits need to be weighed.

## 4.4. Authentication

To comply with the requirement to PK-enable authentication, organizations must configure IdAM solutions to require PIV card authentication for all users, especially privileged users. A wide range of tools and technologies can be used to support PIV authentication to networks, applications, and/or services. For applications that do not natively support smart cards for authentication, an alternate multifactor authentication solution may be needed. Another option is to use a PK-enabled authentication gateway service to broker authentication actions with applications or services that do not offer native support for PIV smart card authentication.

## 4.5. Network Segmentation

Delineation of physical and logical security boundaries for the HVA and supporting network(s) can help organizations tailor security policies, contain the effects of compromises, and reduce recovery activities. Both DMZs and VLANs can provide effective network segmentation.

DMZs create distinct subnetworks for isolating publicly accessible servers and services (e.g., web applications, email gateways) from internal and/or unrelated assets (e.g., workstations, printers). Commercial firewall technologies provide this capability. Firewalls are available as hardware or software solutions, at a wide range of price points, for virtualized and legacy networks. Firewalls with more complex features (e.g., deep packet inspection of application-layer traffic, application proxy functionality, data loss prevention) are generally more expensive than those providing basic port, protocol, and service filtering. For segmentation to be effective, customized access controls with DAPE policies (for both ingress and egress communications) must be applied at each physical and logical boundary.

VLANs can be used to organize endpoints into functional groups (e.g., workstations, printers, servers, voice, video teleconference) and security groups (e.g., test and development assets, wireless devices). Network switches/routers can be configured to prevent unnecessary/unauthorized communication between network segments using access control lists. In terms of costs, organizations may need to consider if a centralized management solution is necessary to achieve effective change management for network infrastructure configurations.

Segmenting network communications can also provide protection capabilities. A VPN can protect the confidentiality of HVA communications by creating a secure tunnel through an otherwise insecure network. Site-to-site VPNs can be created using hardware solutions, while end-user VPN capabilities generally use software solutions. Using dedicated management networks for system management activities (e.g., patching, scanning, auditing, and other system administration tasks) segments security and administration communications from production traffic. This type of segmentation can be particularly effective when management activities are performed using a physically separate, out-of-band network. Using a web proxy for outbound web-based requests is another solution for segmenting network communications. A web proxy can significantly reduce the need for endpoints to communicate directly with external networks, as well as prevent websites from tracking individual endpoint activities. Web proxies provide additional endpoint protections through the application of content

filtering policies (e.g., preventing access to known malware sites, inappropriate content, unauthorized file downloads).

# 5. TRENDS AND EMERGING TECHNICAL SOLUTIONS

Technology to shore up defenses in the areas most critical for HVAs generally exists. Several effective or emerging defenses have been noted above, which are listed below.

- fine-grained attribute based access control
- domain name service security and related standards (e.g., DKIM, Domain Message Authentication Reporting and Conformance)
- whitelisting
- sandboxing

These technologies are generally relevant to long-term plans for HVA upgrades. With planning, these protections can be implemented in the most cost-effective manner available. Emerging technologies for organizations to stay abreast of include those listed below.

- anomaly detection
- continuous diagnostics and mitigation
- ongoing authorization
- integrated threat intelligence

When evaluating emerging defenses, HVA system owners should pay attention to a solution's effectiveness and its ability to integrate with other defenses.

Implementing these defenses involves a number of challenges. Primary among them is the fact that because many government HVA systems are old (legacy), integrating or layering on newer technologies is often either very expensive or impractical (e.g., a completely customized implementation of a technology may have to be implemented, or interfaces between the HVA and new security tool could require changes to the security technology that are impractical or not cost-effective, or that the vendor is unwilling to make).

## 5.1. Threat Modeling

Threat modeling can organically improve security at organizations. Threat modeling is a process for identifying and addressing cybersecurity issues (e.g., threats, vulnerabilities, attack vectors) early in the developmental life cycle based on knowledge of the system's design and underlying network architecture. It can be done while preparing to deploy or build a system and to strategically think about what might go wrong, with the end result being to deliver recommendations on how to mitigate high-risk threats through design modifications and/or configuration changes.

Threat modeling enables cybersecurity personnel to identify, quantify, and address a system's security risks. It also allows programs to make informed choices on how best to improve a system's security posture and resilience while also influencing programs early in the life cycle, when the cost of change is less. Looking at threats from the threat actor's perspective provides a means to identify threats proactively instead of waiting for something to happen and then reacting to it.

There are several threat models and system development life cycle approaches that organizations can implement. Appendix B provides links to some of the most popular threat models.

# 6. SECURITY COST/BENEFIT

The cost of implementing strong cybersecurity can be significant. The costs of suffering a breach due to lack of strong cybersecurity can be even higher, but are less certain.

While no amount of investment in cybersecurity can guarantee that HVAs are completely secure, the costs of suffering and recovering from a cyber-attack are usually much greater than the costs of preparing a defense before the attack happens. By definition, for an HVA, the calculus is further skewed toward investing in defense because the ramifications of a successful attack are greater than average.

As a recent example, the 2015 Office of Personnel Management (OPM) breach caused OPM to contract out for $133 million in credit monitoring services for those affected, with options that would double that amount. One defense, encrypting the PII while at rest, would not have stopped the breach, but would have made the stolen information useless. Such encryption is built into modern operating systems at no additional charge, and more comprehensive solutions can be purchased from other vendors. (OPM is running legacy systems that may require customized, more expensive solutions to enable them to use at-rest encryption. However, we still estimate that such changes would cost significantly less than recovering from a future breach.)

Note that the cost of credit monitoring is only part of the overall cost of the breach to the government and the country. Although the reputational cost is difficult to quantify, it is important to try to account for it. And the long-term costs could escalate, since it is unknown what the attackers might do with the stolen data. (Some arguments have been made to the contrary in the case of private sector breaches, such as Target, Sony, and Home Depot. That is, some have argued that the cost of the breach to the company is less than the company would have paid to invest in deterrent technology. These arguments tend to focus only on the costs to the company that was attacked and do not factor in costs borne by other entities, such as insurance companies, that share the costs of the attack with the victims.)

# 7. SECURITY CHARACTERISTICS AND CONTROL MAPPING

The tables below list the CSF categories and subcategories that are discussed in Section 3, along with a mapping to the HVA overlay. If a CSF subcategory does not map to an HVA overlay control, a reference is made to the appropriate NIST SP 800-53 Rev. 5 control to provide additional guidance. In addition, for each CSF subcategory a mapping was made to the NICE Cybersecurity Workforce Framework, NIST SP 800-181, to show suggested work roles needed to implement and maintain the CSF subcategory.

## Table 1. CSF Categories for Risk Management Mapped to HVA Overlay

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| Identify | Asset Management | ID.AM-3: Organizational communication and data flows are mapped. | CA-3, CA-9 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., intrusion detection system [IDS] alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | Risk Assessment | ID.RA-4: Potential business impacts and likelihoods are identified. | PM-9 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | | ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. | RA-3 | Information Systems Security Developer | Designs, develops, tests, and evaluates information system security throughout the systems development life cycle |
| | Risk Management Strategy | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders. | PM-9 | Executive Cyber Leadership | Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations |
| | | ID.RM-2: Organizational risk tolerance is determined and clearly expressed. | PM-9 | Privacy Officer/Privacy Compliance Manager | Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams |
| Protect | Information Protection Processes and Procedures | PR.IP-7: Protection processes are continuously improved. | PL-2 | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave |
| | Protective Technology | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. | AU Family | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |
| Detect | Anomalies and Events | DE.AE-2: Detected events are analyzed to understand attack targets and methods. | AU-6, CA-7, IR-4, SI-4 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors. | AU-6, CA-7, IR-4, IR-5, SI-4 | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |
| Respond | Analysis | RS.AN-1: Notifications from detection systems are investigated. | AU-6, CA-7, IR-4, IR-5, SI-4 | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |

## Table 2. CSF Categories for Patch Management Mapped to HVA Overlay

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| Identify | Asset Management | ID.AM-1: Physical devices and systems within the organization are inventoried. | CM-8 | Technical Support Specialist | Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable) |
| | | ID.AM-2: Software platforms and applications within the organization are inventoried. | CM-8 | Technical Support Specialist | Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable) |
| | Risk Assessment | ID.RA-1: Asset vulnerabilities are identified and documented. | SI-2, CA-7 | Mission Assessment Specialist | Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness |
| | | ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources. | SI-5 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| Protect | Data Security | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. | CM-8 | Technical Support Specialist | Provides technical support to customers who need assistance utilizing client level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable) |
| | | PR.DS-7: The development and testing environment(s) are separate from the production environment. | CM-2 | Information Systems Security Developer | Designs, develops, tests, and evaluates information system security throughout the systems development life cycle |
| | Information Protection Processes and Procedures | PR.IP-4: Backups of information are conducted, maintained, and tested periodically. | CP-4, CP-9 | Information Systems Security Developer | Designs, develops, tests, and evaluates information system security throughout the systems development life cycle |
| | | PR.IP-12: A vulnerability management plan is developed and implemented. | SI-2 | Information Systems Security Developer | Designs, develops, tests, and evaluates information system security throughout the systems development life cycle |

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| **Detect** | Security Continuous Monitoring | DE.CM-8: Vulnerability scans are performed. | RA-5 | Systems Security Analyst | Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security |
| **Respond** | Mitigation | RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks. | CA-7, RA-5 | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |

## Table 3. CSF Categories for Malware Defense and Anti-Phishing Mapped to HVA Overlay

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| **Protect** | Awareness and Training | PR.AT-1: All users are informed and trained. | AT-2 | Cyber Instructor | Develops and conducts training or education of personnel within cyber domain |
| **Detect** | Anomalies and Events | DE.AE-2: Detected events are analyzed to understand attack targets and methods. | AU-6, CA-7, IR-4, SI-4 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | Security Continuous Monitoring | DE.CM-4: Malicious code is detected. | SI-3 | Cyber Defense Forensics Analyst | Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation |
| | Detection Processes | DE.DP-3: Detection processes are tested. | CA-7, SI-3, SI-4 | System Test & Evaluation Specialist | Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results |
| **Respond** | Mitigation | RS.MI: Activities are performed to prevent expression of an event, mitigate its effects, and eradicate the incident. | IR-4 | Systems Security Analyst | Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security |
| | | RS.CO-2: Events are reported consistent with established criteria. | AU-6 | Cyber Defense Forensics Analyst | Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation |
| | Analysis | RS.AN-1: Notifications from detection systems are investigated. | AU-6, CA-7, IR-4, IR-5, SI-4 | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| Recover | Recovery Planning | RC.RP-1: Recovery plan is executed during or after an event. | CP-10 | System Administrator | Responsible for setting up and maintaining a system or specific components of a system (e.g., installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures) |
| | Improvements | RC.IM-1: Recovery plans incorporate lessons learned. | CP-10 | Cyber Intel Planner | Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace. |

## Table 4. CSF Categories for Access Controls Mapped to HVA Overlay

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| Identify | Governance | ID.GV-1: Organizational information security policy is established. | -1 controls from all families | Cyber Policy and Strategy Planner | Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance |
| | | ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners. | PM-1, PS-7 | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave |
| Protect | Access Control | PR.AC-1: Identities and Credentials are managed for authorized devices and users. | AC-2, IA Family | Product Support Manager | Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components |
| | | PR.AC-3: Remote Access is managed. | AC-17, AC-20 | Product Support Manager | Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components |

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| | Protective Technology | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. | AU Family | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |
| | Awareness and Training | PR.AT-1: All users are informed and trained. | AT-2 | Cyber Instructor | Develops and conducts training or education of personnel within cyber domain |
| | | PR.AT-2: Privileged users understand roles & responsibilities. | AT-3 | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave |
| | | PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities. | SA-9 | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave |
| **Detect** | Security Continuous Monitoring | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed. | CA-7, CM-8, SI-4 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| **Respond** | Communication | RS.CO-1: Personnel know their roles and order of operations when a response is needed. | CP-2, CP-3, IR-3, IR-8 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | | RS.CO-2: Events are reported consistent with established criteria. | AU-6 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | Analysis | RS.AN-1: Notifications from detection systems are investigated. | AU-6, CA-7, IR-4, IR-5, SI-4 | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |

## Table 5. CSF Categories for Authentication Mapped to HVA Overlay

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| **Protect** | Access Control | PR.AC-1: Identities and Credentials are managed for authorized devices and users. | AC-2, IA Family | Product Support Manager | Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components |

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| | Protective Technology | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. | AU Family | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |
| | Awareness and Training | PR.AT-1: All users are informed and trained. | AT-2 | Cyber Instructor | Develops and conducts training or education of personnel within the cyber domain |
| | | PR.AT-2: Privileged users understand roles & responsibilities. | AT-3 | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave |
| | | PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities. | PS-7, SA-9 | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave |
| **Detect** | Security Continuous Monitoring | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed. | CA-7, CM-8, SI-4 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| **Respond** | Communication | RS.CO-1: Personnel know their roles and order of operations when a response is needed. | CP-2, CP-3, IR-3, IR-8 | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave |
| | | RS.CO-2: Events are reported consistent with established criteria. | AU-6 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | Analysis | RS.AN-1: Notifications from detection systems are investigated. | AU-6, CA-7, IR-4, IR-5, SI-4 | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave |

**Table 6. CSF Categories for Network Segmentation Mapped to HVA Overlay**

| Core Function | Category | Subcategory | HVA Overlay Reference or 800-53 Control | Suggested Work Role from NICE Framework | Work Role Definition from NICE Framework |
|---|---|---|---|---|---|
| **Identify** | Asset Management | ID.AM-3: Organizational communication and data flows are mapped. | AC-4, CA-3, CA-9, PL-8 | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats |
| | | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. | PM-1, PM-2 | Product Support Manager | Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components |
| **Protect** | Access Control | PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate. | AC-4, SC-7 | Security Architect | Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes |

# 8. RELEVANT STANDARDS, POLICIES, OR LAWS SPECIFIC TO FEDERAL AGENCIES

- OMB memorandum M-17-09 Management of Federal High Value Assets (https://policy.cio.gov/hva/) 12/9/2016 or its successor. This memorandum contains general guidance for the planning, identification, categorization, prioritization, reporting, assessment, and remediation of federal high value assets.
- OMB memorandum M-16-04 Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government 10/30/2015.
- Executive Order 13636 Improving Critical Infrastructure Cybersecurity. https://www.gsa.gov/portal/content/176547.
- Executive Order 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.
- Federal Information Security Modernization Act of 2014. https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.
- OMB circular A-130.
- Department of Homeland Security Binding Operational Directive 18-02. https://cyber.dhs.gov/bod/18-02/

# APPENDIX A. ACRONYMS

| | |
|---|---|
| **ABAC** | Attribute-Based Access Control |
| **AO** | Authorizing Official |
| **API** | Application Programming Interface |
| **ASCII** | American Standard Code for Information Interchange |
| **AWL** | Application Whitelisting |
| **BIOS** | Basic Input/Output System |
| **BOD** | Binding Operational Directive |
| **CA** | Certification Authority |
| **CAP** | Cross-Agency Priority |
| **CCP** | Common Control Provider |
| **CDM** | Continuous Diagnostics and Mitigation |
| **CD-R** | Compact Disk-Recordable |
| **CFO** | Chief Financial Officer |
| **CIO** | Chief Information Officer |
| **CPU** | Central Processing Unit |
| **CRL** | Certificate Revocation List |
| **CSF** | Cybersecurity Framework |
| **CSIP** | Cybersecurity Strategy and Implementation Plan |
| **CVE** | Common Vulnerabilities and Exposures |
| **DANE** | DNS-based Authentication of Named Entities |
| **DAPE** | Deny-All, Permit-by-Exception |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DHS** | Department of Homeland Security |
| **DKIM** | DomainKeys Identified Mail |
| **DLL** | Dynamic Link Library |
| **DMZ** | Demilitarized Zone |
| **DNS** | Domain Name System |
| **DVD-R** | Digital Video Disk-Recordable |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **ESB** | Enterprise Service Bus |
| **FICAM** | Federal Identity Credential and Access Management |
| **FIPS Pub** | Federal Information Processing Standard Publication |
| **FISMA** | Federal Information Security Modernization Act |
| **GAO** | Government Accountability Office |
| **GSA** | General Services Administration |
| **HIDS** | Host Intrusion Detection System |
| **HIPS** | Host Intrusion Prevention System |
| **HSM** | Hardware Security Module |
| **HSPD** | Homeland Security Presidential Directive |
| **HVA** | High Value Asset |
| **IANA** | Internet Assigned Numbers Authority |
| **ICAM** | Identity Credential and Access Management |
| **IdAM** | Identity and Access Management |
| **IDS** | Intrusion Detection System |
| **IP** | Internet Protocol |
| **IPS** | Intrusion Prevention System |
| **IPv4** | Internet Protocol Version 4 |
| **Ipv6** | Internet Protocol Version 6 |

| | |
|---|---|
| **ISCM** | Information Security Continuous Monitoring |
| **IT** | Information Technology |
| **LAN** | Local Area Network |
| **LDAP** | Lightweight Directory Access Protocol |
| **MAC** | Mandatory Access Control/ Media Access Control |
| **MX** | Mail Exchange |
| **NAC** | Network Access Control |
| **NAS** | Network-Attached Storage |
| **NAT** | Network Address Translation |
| **NetMon** | Network Monitor |
| **NFV** | Network Function Virtualization |
| **NICE** | National Initiative for Cybersecurity Education |
| **NIST** | National Institute of Standards and Technology |
| **NOC** | Network Operations Center |
| **NPE** | Non-Person Entity |
| **NSOC** | Network Security Operations Centers |
| **OCSP** | Online Certificate Status Protocol |
| **OMB** | Office of Management and Budget |
| **OPM** | Office of Personnel Management |
| **OS** | Operating System |
| **OSI** | Open System Interconnection |
| **OTP** | One-Time Password |
| **PAM** | Privileged Access Management |
| **PDU** | Protocol Data Unit |
| **PII** | Personally Identifiable Information |
| **PIN** | Personal Identification Number |
| **PIV** | Personal Identity Verification |
| **PK** | Public Key |
| **PKI** | Public Key Infrastructure |
| **PM** | Program Management |
| **POA&M** | Plan of Action and Milestones |
| **RA** | Risk Assessment |
| **RBAC** | Role-Based Access Control |
| **RF** | Radio Frequency |
| **RMF** | Risk Management Framework |
| **RP** | Relying Party |
| **RSA** | Rivest–Shamir–Adleman |
| **SAN** | Storage Area Network |
| **SAORM** | Senior Agency Official for Records Management |
| **SCI** | Sensitive Compartmented Information |
| **SDN** | Software-Defined Networking |
| **SHA** | Secure Hash Algorithm |
| **SIEM** | Security Information and Event Management |
| **SMTP** | Simple Mail Transport Protocol |
| **SNMP** | Simple Network Management Protocol |
| **SP** | Special Publication |
| **STIX** | Structured Threat Information eXpression |
| **TAXII** | Trusted Automated eXchange of Indicator Information |
| **TCP** | Transport Control Protocol |
| **TLS** | Transport Layer Security |
| **TPM** | Trusted Platform Module |

| | |
|---|---|
| **UDP** | User Datagram Protocol |
| **URL** | Uniform Resource Locater |
| **USB** | Universal Serial Bus |
| **US-CERT** | United States Computer Emergency Readiness Team |
| **VLAN** | Virtual Local Area Network |
| **VM** | Virtual Machine |
| **VMM** | Virtual Machine Monitor |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |
| **WORM** | Write Once Read Many |

# APPENDIX B. REFERENCES

**Business Environment**

- NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

**Risk Assessment**

- SP 800-150: Guide to Cyber Threat Information Sharing.
- SP 800-30 Rev. 1: Guide for Conducting Risk Assessments.

**Risk Management Strategy**

- SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.
- SP 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.

**Threat Modeling**

- SP 800-154 DRAFT: Guide to Data-Centric System Threat Modeling

**Access Control**

- NIST SP 800-162: Guide to Attribute Based Access Control Definition and Considerations.
- NIST SP 1800-3: DRAFT Attribute Based Access Control.
- OMB Memorandum M-04-04: E-Authentication Guidance for Federal Agencies.
- NIST SP 800-63-2: Electronic Authentication Guideline.
- NISTIR 7966: Security of Interactive and Automated Access Management Using Secure Shell (SSH).
- NIST Cybersecurity White Paper: Best Practices for Privileged User PIV Authentication.

**Awareness and Training**

- NIST SP 800-50: Building an Information Technology Security Awareness and Training Program.

**Data Security**

- Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information.
- OMB Memorandum M-06-16: Protection of Sensitive Agency Information.
- OMB Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information.
- OMB Memorandum M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information.
- NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems.

- CNSSI N0. 1253F, Attachment 6, Privacy Overlay.
- HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework.
- NIST SP 800-171 Rev.1: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.
- NIST SP 800-175A: Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies.
- NIST SP 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.
- SP 800-52 Rev. 1: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.
- SP 800-57 Part 1: Recommendation for Key Management, Part 1: General.
- SP 800-57 Part 2: Recommendation for Key Management, Part 2: Best Practices for Key Management Organization.
- SP 800-57 Part 3: Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance.
- NIST SP 800-152: A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS).

**Information Protection Processes and Procedures**

- NIST SP 800-160: Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.
- NIST SP 800-34 Rev.1: Contingency Planning Guide for Federal Information Systems.
- NIST SP 800-184: DRAFT Guide for Cybersecurity Event Recovery.
- NIST SP 800-152: A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS).
- SP 800-88 Rev.1: Guidelines for Media Sanitization.
- SP 800-64 Rev.2: Security Considerations in the System Development Life Cycle.
- DHS Binding Operational Directive 15-01, Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems.
- NIST SP 800-40 Rev. 3: Guide to Enterprise Patch Management Technologies.
- NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems.

**Protective Technology**

- NIST SP 800-95: Guide to Secure Web Services.
- NIST SP 800-47: Security Guide for Interconnecting Information Technology Systems.
- NIST SP 800-167: Guide to Application Whitelisting.
- NIST SP 800-123: Guide to General Server Security.
- DHS Binding Operational Directive 15-01, Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems.
- SP 800-147B: BIOS Protection Guidelines for Servers.
- SP 800-147: BIOS Protection Guidelines.
- SP 800-81-2: Secure Domain Name System (DNS) Deployment Guide.
- SP 800-41 Rev.1: Guidelines on Firewalls and Firewall Policy.
- NIST SP 800-177 Draft: Trustworthy Email.

**Anomalies and Events**

- SP 800-92: Guide to Computer Security Log Management.
- NSA IAD Whitepaper: Spotting the Adversary with Windows Event Log Monitoring.

**Security Continuous Monitoring**

- SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

**Response Planning**

- SP 800-61 Rev. 2: Computer Security Incident Handling Guide.

**Analysis**

- SP 800-86: Guide to Integrating Forensic Techniques into Incident Response.

**Mitigation**

- SP 800-83 Rev. 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
- NCCoE Data Integrity Project: Recovering from a destructive malware attack.

---

[i] "Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems," US Government Accountability Office, GAO 16-501, May 2016, https://www.gao.gov/assets/680/677293.pdf

[ii] "Federal Chief Information Security Officers Opportunities Exist to Improve Roles and Address Challenges to Authority," US Government Accountability Office, GAO 16-686, August 2016, http://www.gao.gov/assets/680/679271.pdf

[iii] "Federal Information Security Agencies Need to Correct Weaknesses and Fully Implement Security Programs," US Government Accountability Office, GAO 15-714, September 2015, http://www.gao.gov/assets/680/672801.pdf

[iv] "Federal Information Security Actions Needed to Address Challenges," US Government Accountability Office , GAO 16-885T, September 2016, http://www.gao.gov/assets/680/679877.pdf

[v] "Guide for Applying the Risk Management Framework to Federal Information Systems," National Institute of Standards and Technology, NIST Special Publication 800-37, February 2010, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

[vi] "IT Scenario Analysis in Enterprise Risk Management," ISACA, ISACA Journal Volume 2, 2011, https://www.isaca.org/Journal/archives/2011/Volume-2/Documents/jpdf11v2-it-scenario-analysis.pdf

[vii] "Guide for Applying the Risk Management Framework to Federal Information Systems," National Institute of Standards and Technology, NIST Special Publication 800-37, February 2010, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

[viii] "Security Guide for Interconnecting Information Technology Systems," National Institute of Standards and Technology, NIST Special Publication 800-47, August 2002, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf

[ix] "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, NIST Special Publication 800-53, Revision 4, April 2013, http://csrc.nist.gov/publications/PubsSPs.html

[x] "High Value Asset Control Overlay," Department of Homeland Security, November 2017, https://community.max.gov/x/RJQ5JQ

[xi] "Managing Information Security Risk," National Institute of Standards and Technology, NIST Special Publication 800-39, March 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[xii] "Managing Information as a Strategic Resource," Office of Management and Budget, OMB Circular No. A-130, July 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[xiii] "Risk Management Framework: A Lab-Based Approach to Securing Information Systems," James Broad, Synergess, 2013

[xiv] "Security and Privacy Controls for Systems and Organizations," National Institute of Standards and Technology, NIST Special Publication 800-53, Revision 5, Pre-release - DRAFT

[xv] "Risk Management Framework for Information Systems and Organizations," National Institute of Standards and Technology, NIST Special Publication 800-37, Revision 2, Discussion DRAFT, September 2017, https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

[xvi] "Guide to Enterprise Patch Management Technologies," National Institute of Standards and Technology, NIST Special Publication 800-40, Revision 3, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[xvii] "Continuous Diagnostics and Mitigation (CDM) Technical Capabilities", Volume Two, Requirements Catalog, Version 1.0, Department of Homeland Security July 18, 2017

[xviii] "Guide to Enterprise Patch Management Technologies," National Institute of Standards and Technology, NIST Special Publication 800-40, Revision 3, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[xix] "Continuous Diagnostics and Mitigation (CDM) Technical Capabilities", Volume Two, Requirements Catalog, Version 1.0, Department of Homeland Security July 18, 2017

[xx] "How the Rise in Non-Targeted Attacks Has Widened the Remediation Gap," Kenna Security, September 2015, https://www.kennasecurity.com/wp-content/uploads/Kenna-NonTargetedAttacksReport.pdf

[xxi] "Critical vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems," DHS BOD 15-01, May 2015
[xxii] "CIS Critical Security Controls: Guidelines," The SANS Institute, Accessed September 2017, https://www.sans.org/critical-security-controls/guidelines
[xxiii] "A Measurement Companion to the CIS Critical Security Controls," Version 6, pg.7, The SANS Institute, October 2015
[xxiv] "Guide to Enterprise Patch Management Technologies," National Institute of Standards and Technology, NIST Special Publication 800-40, Revision 3, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf
[xxv] "High Value Asset Control Overlay," Department of Homeland Security, November 2017, https://community.max.gov/x/RJQ5JQ
[xxvi] "2016 Data Breach Investigations Report," Verizon, April 2016, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
[xxvii] "Continuous Diagnostics and Mitigation (CDM) Technical Capabilities", Volume Two, Requirements Catalog, Version 1.0, Department of Homeland Security July 18, 2017
[xxviii] "A Measurement Companion to the CIS Critical Security Controls," Version 6, pg.14, The SANS Institute, October 2015
[xxix] "High Value Asset Control Overlay," Department of Homeland Security, November 2017, https://community.max.gov/x/RJQ5JQ
[xxx] "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," Committee on Oversight and Government Reform, September 2016, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf