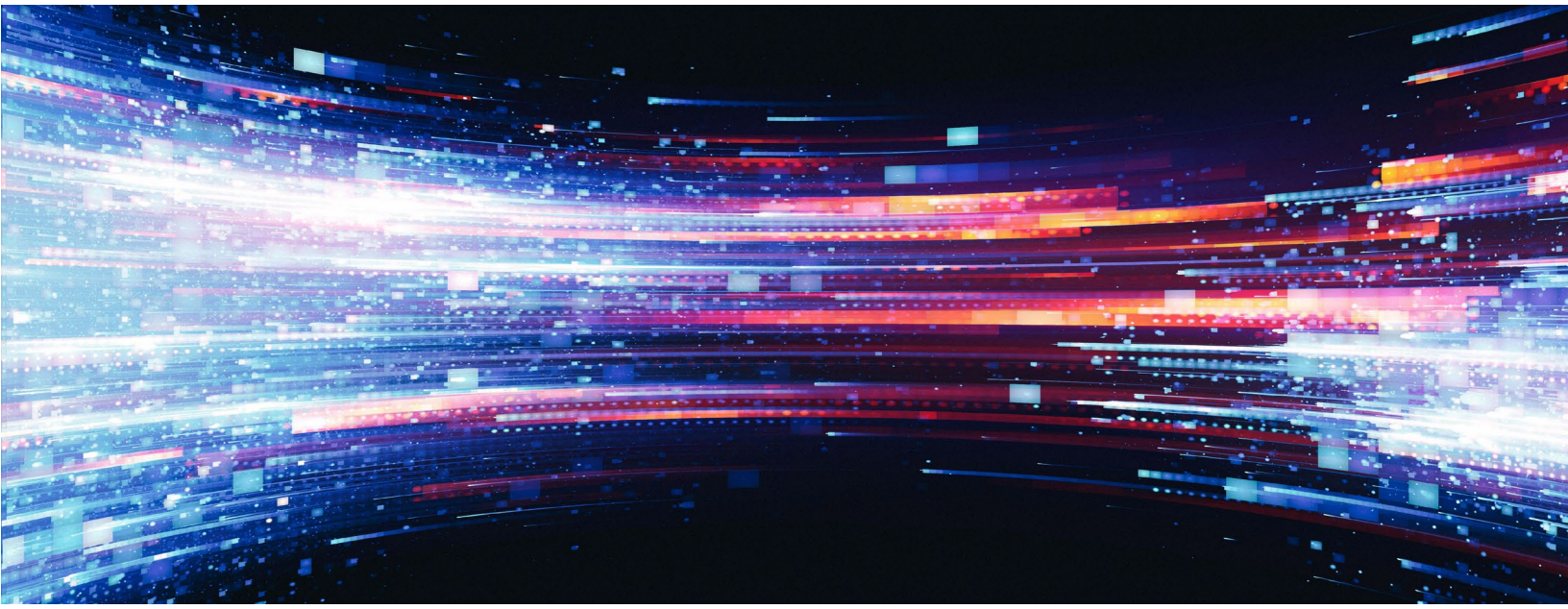

CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

Technical Capabilities

Volume Two: Requirements Catalog

Version 2.4

August 2021

Cybersecurity and Infrastructure Security Agency

RECORD OF CHANGES

Version Number	Date	Revised by	Sections
1.0	07/18/2017	PMO	All
1.4	05/11/2018	PMO	Integrated CDM Phase 4 “How is data protected?” requirements.
2.0	06/30/2020	PMO	All; includes new and refreshed capability sections for Asset Management Capability Area and Network Security Management Capability Area (see Section 1.1.2 for details). Made enhancements to all sections for clarity and consistency.
2.1	09/16/2020	PMO	Minor editorial changes and updates to address Agency comments.
2.2	10/2/2020	PMO	Minor change to page 1: changed “Schedule 70” to “Multiple Award Schedule Information Technology Category (MAS IT)”
2.3	08/11/2021	PMO	All; includes updates to the Common Requirements and Asset Management and Identity and Access Management Capability Areas (see Section 1.1.2 for details).
2.4	8/18/2021	PMO	Added Endpoint Detection and Response (EDR) details (see Sections 2.4.2 and 2.4.2.2.6). Other minor editorial changes.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1 INTRODUCTION

Strengthening the security posture of Federal networks, systems, and data is one of the most important challenges we face as a nation. In response, the Department of Homeland Security (DHS) seeks to provide agencies with the Continuous Diagnostics and Mitigation (CDM) program to safeguard, secure, and strengthen cyberspace and the security posture of Federal networks in an environment where cyber-attacks are continuously growing and evolving.

This document describes the requirements for the CDM program that are consistent with the overarching goal of enabling U.S. Government entities to assess and improve the security posture of Agency information systems. These requirements will be used for CDM solicitations called Dynamically Evolving Federal Enterprise Network Defense (DEFEND) task orders, included as part of DEFEND integration contractor efforts post-award and for ongoing updates to the General Services Administration (GSA) Multiple Award Schedule Information Technology (MAS IT) Category CDM Tools Special Item Number (SIN) Approved Products List (APL). These requirements are commonly used in discrete tasks or engineering activities [often called Requests for Service (RFS)] within the DEFEND task orders, which implement CDM capabilities at agencies and ultimately mature the CDM solutions deployed.

The CDM approach to improve the cyber resiliency of each information system is through an iterative integration strategy that selects and deploys technologies to fulfill a set of security controls (referred to in the program as Capabilities) into the solutions deployed on Agency networks. Figure 1 shows each capability aggregated into a Capability Area (formerly known as phases) that has an underlying security focus area (devices, users, networks, and data).

Figure 1. CDM Capability Areas

The Capability Areas of the program are defined as follows, itemized into subordinate capabilities:

- Asset Management – Capability Area that addresses "What is on the network?" and all Information Technology (IT) assets, including Hardware Asset Management (HWAM) and Software Asset Management (SWAM) assets. Asset Management also includes asset Configuration Settings Management (CSM), Vulnerability Management (VUL), Enterprise Mobility Management (EMM), and Mobile Threat Defense (MTD).

- **Identity and Access Management (IdAM)** – Capability Area that addresses "Who is on the network" and consists of related capabilities that support the IdAM security discipline (i.e., TRUST, BEHAVE, CRED, PRIV). IdAM provides identity proofing and authentication aspects under identity management. It also supports the use, maintenance, and protection of sensitive resources (e.g., data, systems).
- **Network Security Management (NSM)** – Capability Area that addresses "What is happening on the network?", the security of the network, and the resources connected to it. NSM consists of the following complementary capabilities:
    - **Boundary Protection (BOUND)** – Capability that provides network boundary protections that support the NSM key program area. Specifically, BOUND is entrusted with providing network security capabilities to prevent and mitigate any unauthorized network or data access.
    - **Manage Events (MNGEVT)** – Capability that gathers threat data from appropriate sources, identifies security incidents through analysis of data, and performs initial vulnerability assessment impact analyses. MNGEVT is responsible for preparing for security events/incidents.
    - **Operate, Monitor, and Improve (OMI)** – Capability that is responsible for detailed investigation of security incidents, analyzing threat sources and behavior, identifying security root causes through analysis and analytics, determining best mitigation approaches, assessing vulnerability impacts, and evaluating the effectiveness of mitigation options.
    - **Design and Build in Security (DBS)** – Capability that supports cybersecurity practices for developing and deploying software/systems throughout the engineering lifecycle while mitigating the risks of including exploitable vulnerabilities.
- **Data Protection Management (DPM)** – Capability Area that addresses "How is data protected?" and manages the protection of data through the following capabilities: data discovery/classification (DATA_DISCOV), data protection (DATA_PROT), data loss prevention (DATA_DLP), data breach/spillage mitigation (DATA_SPIL), and information rights management (DATA_IRM).

In addition to individual capabilities within Capability Areas, many capabilities are further broken down into sub-capabilities (often simply referred to as capabilities) that are intended to be aligned with industry-recognized technology segments [e.g., Network Access Control (NAC) sub-capability under the BOUND capability]. By decomposing these capabilities in this way, the program can create more manageable cost and technical portions that are achievable with smaller contract vehicles (e.g., using the RFS process), resulting in less complex integrations.

1.1 About this Document

This *CDM Technical Capabilities Volume Two: Requirements Catalog* (henceforth referred to simply as "Volume Two") document represents the functional requirements of the tools and technologies (i.e., Layer A of the CDM Architecture) in scope of the program, aggregated by capability. It is a living document and is intended, along with its supporting technical artifacts (CDM Key Cross-References; see Section 3.1), to satisfy the needs for the program to continuously update the technical baseline of the program, in accordance with Office of Management and Budget (OMB) requirements.[1] A formal document will be published, on a yearly schedule, based on iterative changes and requirements development work contained within the CDM program's Requirements Management System (RMS), which is continuously ongoing.

[1] OMB Memorandum M-20-04, "Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements," 19 November 2019 (available at https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf).

1.1.1 Applicability

Volume Two captures functional requirements for the CDM program.[2] The intent of this artifact is to align capability functions to operational requirements and Key Performance Parameters (KPPs) in the CDM Operational Requirements Document (ORD). Volume Two has two primary uses. First and foremost, it is an engineering baseline, provided to CDM integrators, for use during CDM solution development within contract activities (e.g., using the RFS process). Integrators use this functional requirements baseline to develop, through derivation, a full set of system-level requirements in a Requirements Traceability Matrix (RTM), which will be verified during CDM test events. The RTM defines how the Volume Two requirements will be ultimately met, inclusive of additional deployment considerations such as Agency needs, policies (configurations), and/or environmental constraints. As a secondary use, Volume Two is distributed to tool and vendor stakeholders as the authoritative source for the CDM APL, which contains proposed technologies that are expected to meet CDM requirements.[3] Unless otherwise specified, all requirements apply to the CDM solutions being implemented because this is the functional baseline. Any deviations constitute a baseline change and must be routed through the program's change control board (CCB) for adjudication.

1.1.2 What's New for this Publication

The scope of the fiscal year (FY) 2021 update includes the following:

1. MTD capability added in the Asset Management Capability Area to enable an agency to detect and address malicious mobile applications and network-based attacks.
2. SWAM capability requirements updated to new style (see Section 1.3 for a description of the new style).
3. Application Execution Control (AEC) sub-capability added in the SWAM capability to restrict the installation and execution of software applications based on agency-defined lists of authorized applications.
4. Common requirements updated to new style, and time synchronization requirements added.
5. IdAM Capability Area (TRUST, BEHAVE, CRED, PRIV) updated to new style.
6. Privileged Access Management (PAM) sub-capability added in the PRIV capability to provide a Policy Enforcement Point (PEP) for privileged user access management.
7. Identity Lifecycle Management (ILM) sub-capability added in the PRIV capability to enable automation throughout the IdAM lifecycle by adjusting information in connected repositories to address changing user positions and responsibilities.
8. EMM guidance statements updated for two requirements.
9. Editorial changes made throughout.
10. Changes in Sections 2.4 and 2.5; some instances of "should" changed to "shall".
11. Added Endpoint Detection and Response details in Section 2.4.2; added new Section 2.4.2.2.6.

1.2 Scope

As a Functional Requirements Document (FRD), this document describes requirements in terms of system functions, inputs, and outputs. Functional requirements will trace to one or more ORD requirements (i.e., Operational Requirements). Requirements common to all CDM capabilities appear first, followed by detailed requirements for each individual CDM Capability Area, Capability, and (when applicable) Sub-Capability.

Over time and multiple revisions, the functional requirements in this document will apply to the entirety of the CDM solution (Layers A through D), but the current scope is limited to requirements related to the capabilities that reside in Layer A (i.e., CDM tools and sensors subsystem) of the CDM Architecture.
Figure 2 shows the CDM architecture diagram.

---

[2] The one exception to this currently is the non-functional requirement in the Common Functional Requirements Section (Requirement CMN-7-1) regarding data currency and scalability. Functional scoping is still a principle, and only on rare exceptions are non-functional requirements included to ensure highly desirable properties of the CDM solution that cannot be captured in other artifacts yet.
[3] See the following website for further information: Continuous Diagnostics & Mitigation (CDM) Program | GSA

Accordingly, specific Federal and Agency Dashboard requirements are currently documented through the CDM Dashboard-specific development processes and knowledge management platforms.
Additionally, functional requirements may contain external dependencies or inputs that reside outside the control of the Program Management Office (PMO) and are not explicitly defined in this document. The primary example is when Agency policy is mandated to meet the requirement. Examples include device authorization criteria [e.g., authoritative device list, Federal Information Security Management Act (FISMA) system boundaries] that represent the Agency's desired state or business rules where Agency policy dictates conditions when remediation steps (e.g., denying connections or blocking traffic) are executed. Requirements containing these dependencies must be examined, analyzed, and decomposed when they are employed by DEFEND integrators through acquisition artifacts (i.e., RFS).

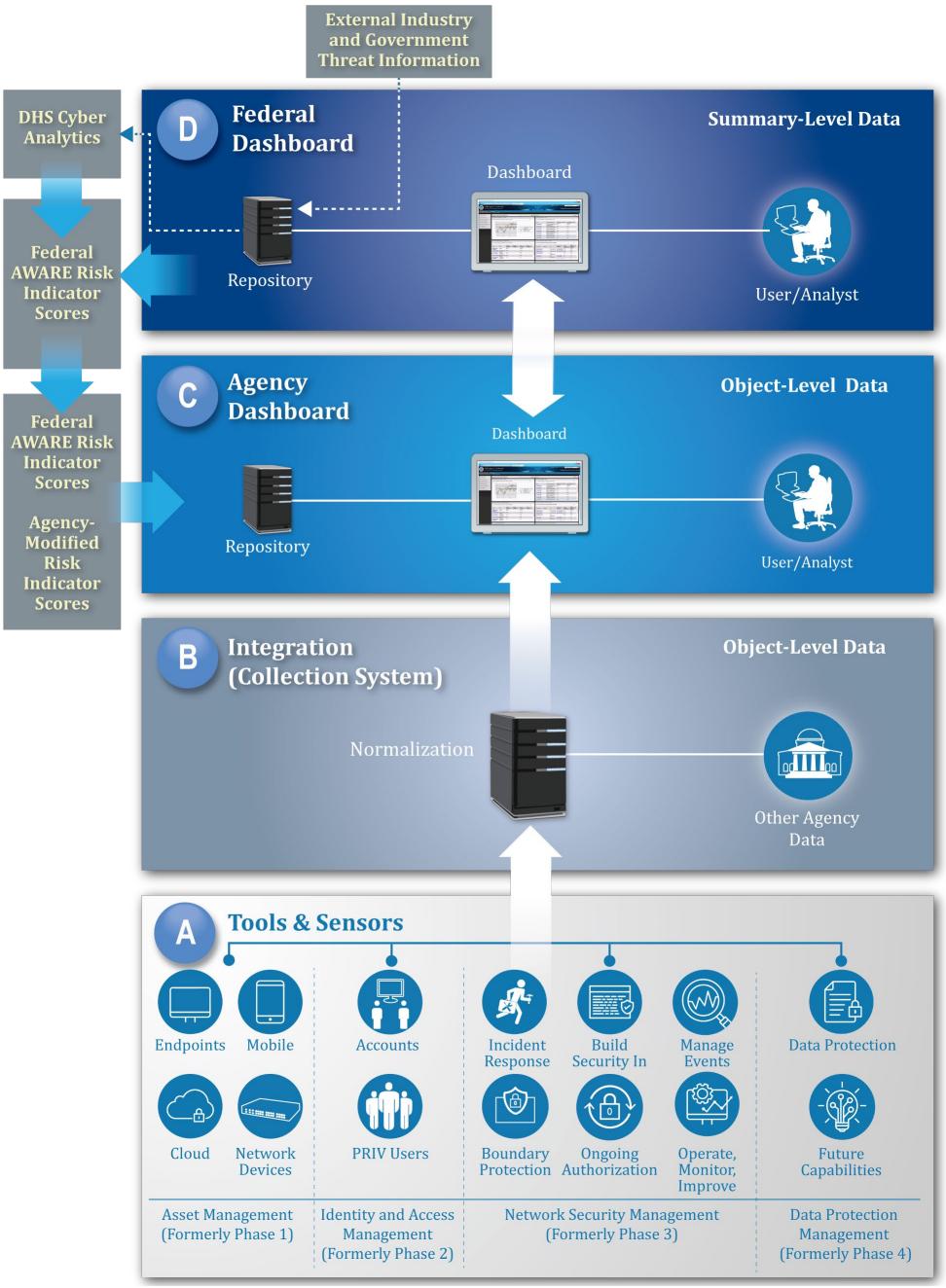

Figure 2. CDM Architecture

Lastly, other items out of scope of this FRD include the following:

- Formal program definitions and terms (see Section 3.1, *CDM Integrated Data Dictionary [AV-2])*
- Specification-level data requirements (see Section 3.1, *CDM Data Model Document, Version 3.8.1*, and the physical implementation by the Dashboard developer, the Dashboard Data Target)
- CDM prescribed or documented requirements management processes
- Instructions or Concept of Operations (CONOPS) of the APL process
- Requirements that do not meet the criteria for Functional requirements (This version maintains Operational Requirements for some capability sections, but those will be replaced by Functional requirements in future versions.)
- Agency-specific requirements or needs (i.e., Agency procedures, tool preferences)
- CDM contractor-specific data integrations techniques and processes that are intended to facilitate CDM Dashboard data integration (i.e., CDM Layer-B tools, technologies, or requirements)

1.3 Requirements Style and Structure

As previously discussed, the requirements in this artifact are written agnostic of agency-specific needs or requirements as those inputs are expected to be solicited during the decomposition and derivation process that results in the RTM. Appropriately, the CDM PMO employs a generic, but consistent, set of verbs and nouns to leave solutions engineering activities unconstrained (i.e., Agency needs elicitation, requirements decomposition and derivation) while clearly communicating functionality (and intent). The only exception to this guideline is in cases where CDM-specific or reserved terminology [e.g., Master Device Record (MDR) or Unauthorized Device] is used. In this scenario, the CDM program's data dictionary (AV-2) is the primary artifact for establishing a common program lexicon and has the authoritative definitions and guidance.

Furthermore, the program supports a principle of allowing agencies and integrators to implement whichever industry tools they feel are most appropriate to their needs, provided they can meet the functional needs of the program. Therefore, the Functional requirements in this document are also vendor-agnostic, allowing industry, agencies, and the CDM integrators to collaborate on technologies they feel are appropriate to the program's baseline (see the APL use case in Section 1.1.1).

Additionally, this document uses a concept referred to as "common" requirements as a way to condense duplicative requirements that apply to all capabilities and, consequently, any tools or sensors that are acquired to support those capabilities. Common requirements should be interpreted as additional requirements for every capability and, as a general principle, are not duplicated or contradicted within each capabilities' specific requirements.

The CDM Program is updating requirements to provide greater engineering clarity and direction. Revisions include the following:

- Identification of functions within a capability, to provide a better understanding of the overall functionality and the requirements, for most capabilities
- A numbering scheme that aligns with the functions
- Guidance statements that are designed to convey additional information relative to the requirement. Guidance statements are for situational awareness and clarifying requirement intent; they are not requirements. Each program requirement contains the word "shall"
- A tool capability table that identifies the tool categories that could potentially provide the required functionality and provides a summary of the tool functionality
  Note: These are presented as a general set of technologies that are used to drive requirements developments against key functionality presented by industry. They are not to be interpreted directly as requirement, which are represented in "shall" statements.

- As applicable, a table of tools that may need to be integrated to provide the required functionality
- Some functional requirements employ the following clause, "When configured by an Administrator". This clause is intended to reflect that the function has to be configured; at a minimum it must be turned on to be operational. The function can be turned off but is required for the capability to be fully instantiated and must be turned on to test. The term 'administrator' will be construed as the CDM system integrator or engineer for purposes of configuring the tool to satisfy the requirement, considering that in some cases the configuration may have been completed in advance by the Agency. Any dependency on Agency policy will be cited explicitly elsewhere in the requirement. By itself, this clause does not allow for any Agency dependency
- Operational requirements are being removed, as the ORD captures operational requirements and Technical Volume Two is the CDM Functional Requirements Document (FRD) Some operational were functional, some were covered by the ORD

Figure 3 shows an example of the new requirements style and structure.

Req. UID	Requirement Text
Enforce Access Control	
NAC-5-1	When configured by the administrator, the NAC capability shall block devices failing network access privilege validation from connecting to the network.
	Guidance: Some agencies may have a policy to block devices, others may quarantine.
NAC-5-2	When configured by the administrator, the NAC capability shall quarantine devices failing network access privilege validation from connecting to the network.
	Guidance: Some agencies may have a policy to block devices, others may quarantine.

Figure 3. New Functional Requirements Style (2020)

As part of the CDM Program's yearly obligation to update the program's baseline, each capability will be revised in this manner on an iterative basis. Capabilities that have not yet been updated will remain in the previous style (employed originally in 2018) until they are updated.

SECTION 2 CDM CAPABILITIES

2.1 Common Requirements

The requirements in this section are common, mandatory, and intended to apply to all CDM capabilities in addition to each capability's unique functional requirements.

References to security data protections include protections and safeguards that may be unique to a given type of sensitive information that is produced, consumed, and/or processed by a CDM capability.

Non-functional requirements in Section 2.1.2 are used to describe constraints and/or characteristics that all CDM capabilities must align to and are not necessarily functions in themselves.

2.1.1 Common Functional Requirements

Table 1. Common Functional Requirements

Req. UID	Requirement Text
CMN-1-1	The CDM capability shall be configured to minimize the operational impact to agency networks based on agency policy.
	Guidance: Agency networks may require the need to minimize the use of network bandwidth and/or minimize the use of endpoint system resources to limit potential impact to mission/business operations. The tools/sensors are intended to be configurable to work around these constraints while maintaining capability effectiveness.

Req. UID	Requirement Text
CMN-2-1	The CDM capability shall record an associated date/time with each instance of Actual State information.
	Guidance: "Actual state information" is a generic term to convey each CDM tool/sensor's observation (if applicable) of a CDM object setting or state that is relevant to a potential defect or inventory of interest to the CDM program. The intent of this requirement is to ensure all capabilities can timestamp data/observed events to ensure it is available for CDM Dashboard reporting, if required.
CMN-2-2	The CDM capability shall identify the source of Actual State information.
	Guidance: "Source" can be interpreted as either a CDM object (device, user) and/or the source that is authoritative (incident repository) for the purposes of the CDM system and its data need.
CMN-2-3	The CDM capability shall use time obtained from an Agency Authoritative Time Server for timestamps for Actual State information.
	Guidance: "Actual state information" is all mission-essential information produced by CDM tools/sensors including audit records. Agency Authoritative Time Servers are intended to be existing infrastructure provided by the Agency.
CMN-2-4	The CDM capability shall use secure authentication to connect to Agency Authoritative Time Servers based on agency policy
	Guidance: This is to prevent time sources from being spoofed or otherwise manipulated maliciously. Secure authentication is either using a pre-shared secret or public/private keys. In some cases, tools may inherit secure time synchronization from an acceptable host server time synchronization implementation.
CMN-2-5	The CDM capability shall preserve timestamps recorded in Actual State information in any subsequent processing of the information
	Guidance: "Actual state information" is all mission-essential information produced by CDM tools/sensors including audit records. For CDM a "timestamp" includes date (MM, DD, YYYY) and time at the granularity specified in CMN-2-7.
CMN-2-6	The CDM capability shall use Coordinated Universal Time (UTC) or a local time with local UTC offset identified as such, in timestamps
CMN-2-7	The CDM capability shall record timestamps using a granularity of 1 second.
	Guidance: This is especially important for incident response and for time-ordering audit records. The intent is to allow for granularity of record keeping that allows tracing of correlated events. Granularity of one second or less includes date (MM, DD, YYYY) and HH:MM:SS level detail in the timestamp.
CMN-3-1	The CDM capability shall share (send and receive) information with other CDM capabilities (and other CDM subsystems) in industry-standardized data formats, protocols, and/or application programming interfaces (APIs).
	Guidance: The CDM PMO intends for interoperability between CDM sub-systems and/or capabilities to occur over well defined, open (i.e., non-proprietary) interfaces and protocols (e.g., IP, HTTPS.) that are sustainably supported by industry (e.g., RESTful APIs). Example of standard formats include, but are not limited to JSON, XML, and CSV. The intent of this requirement is to ensure bi-directional, open interoperability.
CMN-3-2	Upon input by the administrator, the CDM capability shall export information in human-readable file formats that minimally include at least one of the following: • Portable Document Format (PDF) • CSV • Microsoft Office formats (.docx, .xlsx, etc.)
CMN-3-3	When configured by the administrator, the CDM capability shall automatically exchange agency and CDM required data, collected by the capability, with other tool platforms, on a scheduled basis.

Req. UID	Requirement Text
	Guidance: The CDM PMO intends to have interoperability between different tool platforms (i.e., CDM tools/sensors) to be automatable (via scheduling). The intent is to support automated reporting and exchange of security relevant information to satisfy CDM PMO and Agency-specific reporting/integration requirements, which are expected to be solicited by the CDM Integrator during the technical planning phases of the engineering lifecycle (i.e., RTM development through requirements derivation). See the CDM Logical Data Model (LDM) or CDM Data target for additional information on CDM required data.
CMN-3-4	When configured by the administrator, the CDM capability shall automatically exchange agency and CDM required data, collected by the capability, with other tool platforms, after a pre-defined trigger event.
	Guidance: The CDM PMO intends to have interoperability between different tool platforms (i.e., CDM tools/sensors) to be automatable (via configured trigger events). The intent is to support automated reporting and exchange of security relevant information to satisfy CDM PMO and Agency-specific reporting/integration requirements, which are expected to be solicited by the CDM Integrator during the technical planning phases of the engineering lifecycle (i.e., RTM development through requirements derivation). See the CDM LDM or CDM Data target for additional information on CDM required data.
CMN-3-5	Upon input by the administrator, the CDM capability shall automatically exchange agency and CDM required data, collected by the capability, with other tool platforms.
	Guidance: CDM PMO intends to have interoperability between different tool platforms (i.e., CDM tools/sensors) to be situationally conducted in an ad-hoc manner. The intent is to support automated reporting and exchange of security relevant information to satisfy CDM PMO and Agency-specific reporting/integration requirements, which are expected to be solicited by the CDM Integrator during the technical planning phases of the engineering lifecycle (i.e., RTM development through requirements derivation). See the CDM LDM or CDM Data target for additional information on CDM required data.
CMN-4-1	The CDM capability shall report CDM-required information on a recurring basis to maintain a data currency requirement of 72 hours or less at the CDM Agency Dashboard subsystem.
	Guidance: This is a key performance parameter that ensures that the CDM data received at the Agency Dashboard is less than or equal to 72 hours from its source. This 72-hour currency requirement pertains to the CDM architectural Layer A (CDM tools/sensors sub-system) and the Layer B (CDM data integration tools) combined. The allocation to each Layer will be performed as part of the integration effort.
CMN-5-1	The CDM capability shall be configurable to retain information for an agency-defined period or 30 days, whichever is lower.
	Guidance: Data retention requirements that go beyond 30 days require CDM PMO approval and may require supplemental infrastructure (i.e., storage, compute).
CMN-6-1	When data encryption is required, based on agency policies, the CDM capability shall encrypt sensitive[4] information transmitted by the capability with FIPS 140-2 or 140-3 validated cryptographic modules.
	Guidance: Federal Information Processing Standard (FIPS) 140-2 has been superseded by FIPS 140-3, effective September 2019.[5] FIPS 140-2 certificates are valid for an additional five years. *This requirement is intended to protect Agency sensitive information that is processed and/or created then transmitted by the capability itself in the course of performing its functions. This may include: privacy data, acquisition sensitive information, CUI, information system security information (e.g., vulnerabilities), etc.*

[4] Sensitive information is information that requires safeguarding or dissemination controls in accordance with law, regulations, and government-wide policies, excluding classified information.
[5] Refer to https://csrc.nist.gov/publications/detail/fips/140/3/final.

Req. UID	Requirement Text
CMN-6-2	When data encryption is required, based on agency policies, the CDM capability shall encrypt sensitive information stored by the capability with FIPS 140-2 or 140-3 validated cryptographic modules.
	Guidance: FIPS 140-2 has been superseded by FIPS 140-3, effective September 2019. FIPS 140-2 certificates are valid for an additional five years. *This requirement is intended to protect Agency sensitive information that is processed and/or created then stored by the capability itself in the course of performing its functions. This may include: privacy data, acquisition sensitive information, CUI, information system security information (e.g., vulnerabilities), etc.*

2.1.2 Common Non-Functional Requirements

Table 2. Common Non-Functional Requirements

Req. UID	Requirement Text
CMN-7-1	The CDM capability shall scale to data growth rates defined by the agency or 25% above the current user and device baseline inventories, whichever is greater.
	Guidance: The intent of this requirement is to ensure the CDM solution can accommodate a moderate amount of growth and still achieve performance requirements regarding data completeness and timeliness (CMN-4-1). "Data Growth Rate" is defined as an (expected) additional amount of CDM-required information (data) that is based on 5-year projections using current statistics regarding federal employment. For CDM solutions that have multiple agencies (e.g., Shared services), the growth rate must include input from all agencies.

2.2 Asset Management Capability Area

Asset Management Capability Area addresses "What is on the Network?' and focuses on identifying and monitoring Agency devices, ensuring that they are properly configured, and vulnerabilities have been identified and remediated. The Asset Management Capability Area consists of the HWAM, SWAM, CSM, VUL, and EMM capabilities.

These functions are briefly summarized below, and the requirements are separately specified later in the HWAM, SWAM, CSM, VUL, and EMM sections.

- HWAM discovers and manages Internet Protocol (IP) addressable devices on the network.
- SWAM discovers and manages the software installed on devices on the network.
- CSM identifies and manages the security configuration settings for devices (and the associated installed software) on the network.
- VUL discovers and supports remediation of the vulnerabilities in software installed on devices on the network.
- EMM secures the use of Agency mobile devices.

2.2.1 Hardware Asset Management (HWAM) Capability

The HWAM capability discovers IP-addressable hardware on a network.
HWAM establishes and maintains an authorized hardware inventory baseline, unique identifiers (UIDs) for hardware, and other properties, such as the manager of the hardware.
HWAM also establishes and maintains the actual inventory of hardware in accordance with data currency requirements, along with information needed to assess the risk to and locate the hardware.
The capability to maintain and update the inventory needs to allow for decentralized administration and only for assets for which they are accountable. Data in the authorized hardware inventory baseline must be validated continuously through automated hardware discovery. Manual processes, such as assigning hardware to the baseline, are expected to integrate with and be supported by automated processes.

The following is a non-exclusive list of tool functionalities that support the HWAM capability:

Tool Category Names	Summary of Functionality
Passive detection tools	Identify devices on the network through non-intrusive means, such as log collection
Tools to interrogate network infrastructure to detect devices	Determine IP addresses on the network, which ports are in use, and how devices on the network are connected
Active scanning tools	Identify devices on the network using active means, such as ping and response methods
Tools that provide packet filtering for device identification	Intercepts, logs, and analyzes network traffic and data

2.2.1.1 HWAM Functional Requirements

This section provides functional requirements for the HWAM capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine-readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 3. HWAM Functional Requirements

Req. UID	Requirement Text
HWAM-1	The HWAM capability shall uniquely identify each device on the Agency network with an identifier that persists across network location changes.
	Guidance: Network location changes include physical or logical changes that would change key Layer 3 and Layer 2 addressing functionality (i.e., different IPv4/IPv6 addresses, different MAC addresses, etc.)
HWAM-2-1	When configured by the administrator, the HWAM capability shall collect inventory information on all IP addressable devices on the Agency network on an automated basis.
	Guidance: Automated HWAM detection may include multiple different engineering approaches such as schedule driven activity (e.g., scheduled scans) or passive detection (e.g., network packet ingestion/detection).
HWAM-2-2	Upon administrator command, the HWAM capability shall scan IP-addressable devices on an ad-hoc basis to collect inventory information for each device on the Agency network.
HWAM-3	When configured by the administrator, the HWAM capability shall record the authorization status of each detected device on the network, based upon an automated comparison of the agency-defined desired state for the network against the collected device data.
	Guidance: Desired State implies a known good state for the network or information system which the HWAM capability operates within. Some examples include an authorized list of devices, an SSP-defined logical boundary of devices, or a set of network architectures to define perimeters.
HWAM-4	The HWAM capability shall maintain a timely, updated device inventory that includes actual state information for each device and each devices authorization status.
	Guidance: Device inventory information includes device type (e.g., router, workstation, firewall, printer), detection times, owner/manager, operational status, and any other explicit dataset called out in the HWAM requirements. Authorized or Unauthorized status indicate whether devices are approved or unapproved, based on an agency policy. For more information refer to the CDM LDM and/or Dashboard Physical Schema.
HWAM-5	The HWAM capability shall classify the type of each device detected on the network.
	Guidance: Refer to the CDM Program Data Dictionary for applicable device categories and types.
HWAM-6-1	The HWAM capability shall collect physical location data for each device detected on the network.
	Guidance: Physical Location data describes data that can be used by administrators to physically locate any device scanned or detected by the HWAM capability.

Req. UID	Requirement Text
HWAM-6-2	When configured by the administrator, the HWAM capability shall authenticate to devices to conduct a scan to collect the ALL of the following information types for each scanned device: • Device subcomponents • Attached peripheral devices • Local accounts and users (to the device)
	Guidance: Attached peripheral devices may include items attached through USB interfaces (e.g., removable USB drives, mice, keyboards, CD/DVD drives, mobile devices, etc.)
HWAM-7	The HWAM capability shall report a device inventory that includes unique device ID, device model, type, manufacturer, OS, authorization status, location, and MDR required attributes.
	Guidance: MDR required attributes is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical and physical data models, data requirement documents). Reported inventories are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards). Authorized or unauthorized status indicates whether devices are approved or unapproved, based on an agency policy.

2.2.2 Software Asset Management (SWAM) Capability

The SWAM capability discovers software installed on devices operating on an Agency's network that are categorized as endpoints.[6] A complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings.

SWAM establishes and maintains a software inventory to include, but not limited to, the following key attributes:

- UIDs that allow analysts to quickly identify specific software running on the network
- Manufacturing information such vendor and product name, as well as versioning information

SWAM also establishes and maintains the actual inventory of all software in accordance with data currency requirements (timely, recurring inventory updates), along with information needed to physically locate the software (i.e., device/MDR associations) in order to enable risk assessment and mitigation activities.

The capability to maintain and update an authoritative software inventory, including attribute information, is intended to satisfy key Federal requirements to manage software within the enterprise, as stipulated in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the NIST 800-53 controls.[7]

The SWAM capability includes the AEC sub-capability, which restricts the installation and execution of software applications that are not authorized to be on the device or information system (per agency policy).
The following are the SWAM functions:

1. **Detect Installed Software** supports the collection of SWAM information on endpoint devices by identifying and detecting installed software through ad-hoc and/or automated scans with credentials sufficient to produce complete and accurate inventories.
2. **Restrict Changes to Authorized Users** requires agency-defined privileges for modification of the SWAM capability's administrative functionality.
3. **Remove Installed Software** removes installed software upon administrative action by an authorized user (e.g., remove installed software detected on an endpoint that is known to be unauthorized or unapproved).

[6] Devices of category ENDPOINT include workstations, laptops, and servers. See the program's AV-2 and the CDM Data Model Document for additional information.
[7] See NIST CSF v1.1 (ID.AM-2: Software platforms and applications within the organization are inventoried) and NIST 800-53 (Control CM-8: Information System Component Inventory) for more information.

4. **Maintain and Report CDM SWAM Data** maintains the inventory of installed software on the Agency network, including actual state information (devices installed on, time detected, etc.) and software component information (software vendor name, product name, and version details). This function also reports on the current software inventory to the CDM dashboards.

The following is a non-exclusive list of general tool functionalities (i.e., tool categories that provide SWAM functional requirements):

Tool Category Names	Summary of Functionality
Software version scanning tools	Collect Information about Installed Software.
Software inventory management tools	Identify all software applications on one or more devices and create software inventory.

The following is a non-exclusive list of tools that SWAM may integrate with:

Tool Category Names	Summary of Functionality
Application (Execution) Control tool	Receive information about changes in Allow/Deny list affecting software inventory. Receive information on unapproved or unauthorized software on devices, based on configured agency policy.
Software deployment tools	Notification of software installed or removed. Notification of unauthorized software detected.

2.2.2.1 SWAM Functional Requirements

This section provides functional requirements for the SWAM capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine-readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 4. SWAM Functional Requirements

Req. UID	Requirement Text
Detect Installed Software	
SWAM-1.1	The SWAM capability shall uniquely identify each instance of installed software that is detected on endpoint devices on the network.
	Guidance: Industry UID standards should be utilized when available but are not required. In the absence of an industry UID, a CDM solution or tool generated UID is acceptable. UID standards include for example, Common Platform Enumeration (CPE) or Software Identification (SWID) Tags for each installed software product to identify instances of software products and components across devices on the network. See the CDM LDM and data dictionary for definitions of UniqueSoftwareID.
SWAM-1-2	When configured by the administrator, the SWAM capability shall scan endpoint devices on the network on an automated basis to detect installed software.
	Guidance: Automated scans may include multiple different engineering approaches such as schedule driven activity (e.g., scheduled scans). See requirements SWAM 5-1 through 5-5 for more information regarding software information.
SWAM-1-3	Upon administrator command, the SWAM capability shall scan endpoint devices on the network to detect installed software on an ad-hoc basis.
SWAM-1-4	The SWAM capability shall authenticate to endpoint devices with privileged access when conducting a scan for installed software.
	Guidance: The privileges required to conduct a successful SWAM scan are CDM solution specific. Note that software inventories acquired by agent-based architectures meet this requirement's intent if they are installed appropriately.

Req. UID	Requirement Text
SWAM-1-5	When executing a scan, the SWAM capability shall detect between 80% (threshold) and 95% (objective) of installed software on endpoint devices on the agency's network.
	Guidance: This requirement traces to CDM ORD objectives, specifically to KPPs 1.1, 1.2. Intent is to ensure that SWAM tools perform in a way such that the # of instances of installed software reported on all devices being scanned divided by the number of instances of known software installed on those devices is greater than or equal to 80%.
SWAM-1-6	When conducting a scan, the SWAM capability shall detect installed software with a false positive rate no greater than 0.1%.
	Guidance: The privileges required to conduct a successful SWAM scan are CDM solution specific. Note that software inventories acquired by agent-based architectures meet this requirement's intent if they are installed appropriately. False positive and False Negative Rates (≤ 0.1%) are defined by the program's Operational Requirements Document (ORD). False positive information is determined by reporting installed software on an endpoint device that is known not to be installed on the endpoint device.
SWAM-1-7	When conducting a scan, the SWAM capability shall detect installed software with a false negative rate no greater than 0.1%.
	Guidance: The privileges required to conduct a successful SWAM scan are CDM solution specific. Note that software inventories acquired by agent-based architectures meet this requirement's intent if they are installed appropriately. False positive and False Negative Rates (≤ 0.1%) are defined by the program's Operational Requirements Document (ORD). False negative information is determined by non-reporting of installed software on an endpoint device that is known to be installed on the endpoint device.
Restrict Changes to Authorized Users	
SWAM-3.1	The SWAM capability shall enforce access control to only allow selected users to perform administrator functions, as defined by agency policy.
	Guidance: Authorized users and agencies roles they align to is expected to be determined by agency policy. What classifies as an administrator function is expected to be determined by agency policy.
Remove Software Upon Request	
SWAM-4.1	When configured by the administrator, the SWAM capability shall remove software installed on endpoint devices on a scheduled time in the future.
	Guidance: The administrator is expected to identify or know what installed software needs to be removed, based on outputs from other capabilities (e.g., from AEC) or a policy list of approved/prohibited software. The amount of time it takes to ultimately remove software is solution dependent. This requirement stipulates the process to uninstall proceeds immediately upon the scheduled time of execution.
SWAM-4-2	Upon administrator command, the SWAM capability shall remove software installed on endpoint devices on an ad-hoc basis.
	Guidance: The administrator is expected to identify or know what installed software needs to be removed, based on outputs from other capabilities (e.g., from AEC) or a policy list of approved/prohibited software. The amount of time it takes to ultimately remove software is solution dependent. This requirement stipulates the process to uninstall proceeds immediately upon administrator command.
Maintain and Report CDM SWAM Data	
SWAM-5-1	When conducting a scan, the SWAM capability shall collect all of the following software component information for all installed software detected on endpoint devices: • Software Product Vendor • Software Product Name • Software Product Version
	Guidance: See the CDM LDM and data dictionary for additional guidance on these data types.

Req. UID	Requirement Text
SWAM-5-2	When conducting a scan, The SWAM capability shall collect all of the following required actual state information for all installed software detected on endpoint devices: • Timestamp of when the software was detected on the endpoint device • Endpoint Device Identifier where product was detected • Type/Classification of Software detected
	Guidance: Endpoint Device Identifier is determined by the CDM solution's design but is intended to identify the device that the software was detected on (e.g., hostname, IP/Mac addresses, etc.). See the CDM LDM and data dictionary for additional guidance on these data types.
SWAM-5-3	The SWAM capability shall continuously maintain a timely, updated inventory of installed software that includes every software UID, all software component information, and all actual state software information for each endpoint device on the agency's network.
	Guidance: See SWAM-5-1 and 5-2 for more information on software component and actual state software information. See SWAM-1-1 for more information on software UIDs. Note that the term "maintains" implies the creation of the software inventory.
SWAM-5-4	The SWAM capability shall report an inventory of installed software that includes every software UID, all software component information, and all actual state software information for each endpoint device on the agency's network.
	Guidance: See SWAM-5-1 and 5-2 for more information on software component and actual state software information. See SWAM-1-1 for more information on software UIDs. Reported inventories are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).

2.2.2.1.1 Application Execution Control Sub-Capability

The AEC restricts the installation and execution of software applications based on agency defined lists of authorized applications (Allow Lists) and/or unauthorized applications (Deny Lists). AEC is a sub-capability under the SWAM capability. AEC uses Allow Lists, Deny Lists, and related agency policy to serve as the PEP for software installation and execution within the CDM solution.

Implementation of the AEC sub-capability is intended to reduce net cyber risk to the confidentiality, integrity and availability of controlled but unclassified (CUI) data supporting Agency business missions by preventing unauthorized application installation or execution in a timely manner.[8] Preventing such execution is expected and intended to reduce overall Agency vulnerability exposure. Further, this sub-capability supplements and offers defense-in-depth alongside existing endpoint protection tools and sensors such that malicious code execution likelihood is reduced and minimized, reports targeted data to the CDM dashboard of the efficacy of Allow List or Deny List implementation for senior risk executives, and enables Allow and/or Deny List automated workflow and orchestration functions to reduce the administrative burden on the user community.

An application Allow List (formerly referred to as whitelist) defines the applications that are authorized by the agency to be installed and executed through some combination of file path, file name, file size, as well as digital signatures and cryptographic hash. There are multiple methodologies for preventing malicious code execution, and each has different requirements with respect to resource investment, addresses different types of threats, and has different success rates depending on organizational factors:[9]

- **Location-Based (or Path-Based):** Allow List specifies a path or multiple paths where software must be located, accompanied by strong file and directory permissions.
- **Certificate-Based:** Also known as "signing," certificates are created to certify that the applications come from a trusted source.

[8] Some AEC requirements use the term cyber relevant time. Cyber relevant time means the mitigating action (e.g., Protect/
Block or Detect) occurs before the threat action has completed. Cyber relevant time is dependent upon the threat action as well as the architecture.
[9] Application Whitelisting (AWL): Strategic Planning Guide, DHS Federal Network Resilience

- **Reputation-Based (or Service-Based):** Many applications have installed, or affiliated services associated with them. States or values (e.g., file hash, URL, IP address) are defined per policy, and then the software assesses, identifies and/or compares the state or value at a given time.
- **Behavior-Based:** Administrators define specific user and system behavior sequences that the behavior-based execution prevention program verifies. For example, if a particular application routinely (and legitimately) spawns new processes or writes to the hard disk.
- **Hash-Based:** A cryptographic hash can be created for a file or groups of files affiliated with an application using commonly accepted protocols.
- **Affected File Types:** In addition to the above choices the methodology may also specify which types of software files will be affected by the Allow/Deny List implementation.

Deny lists (formerly referred to as blacklists) are used to block explicitly unauthorized applications and permit all others. Deny Lists can be used in addition to Allow Lists, or as an alternative.

It can be more efficient for organizations to implement application policies using both the Allow List and Deny List. It is common for an application to be on both the Allow List and Deny List for shared applications with licensing constraints (after the allowed number of installations on a set of endpoints, further installation is to be denied on another set of endpoints) and security policy enforcement (only use particular applications during specific times) that may require action either from a rules-based or administrator-provided input. The agency security policy should be reviewed to ensure that conflicting policy does not exist (e.g., an application appears on the Allow List and Deny List at the same time for the same endpoint) when developing such lists. It is recommended that in the case of conflict between the lists (appears on both lists at the same time), that the default action is to use the Deny List. Organizations may have specific application stores to enable employees to install certain applications (e.g., WebEx) rather than from a public application store.

Agencies' policies are expected to be informed by the criticality of applications (and devices applications are installed on) on agency networks to determine acceptable tolerances around false positive and/or negative rates to minimize operational impacts as the AEC capability is implemented.

AEC control policies are defined to specify what actions are to be taken (log the attempt, notify the user, block the installation, etc.) when an attempt is made to install or execute an application not meeting the agency policy requirements. Different policies may apply to different types of devices. Enterprise Mobility Management (EMM) has cybersecurity for mobile devices (tablets, smartphones, E-readers), while AEC will exclusively scope to cybersecurity for servers, laptops, and workstations that may have different policies (collectively referred to as an "endpoint device" within the functional requirements).[10] Future iterations of this capability will consider broader focus and scope.

It is more practical to implement Allow/Deny Lists on hosts that are centrally managed and have a consistent application workload. Allow/Deny List solutions are generally strongly recommended for hosts in high-risk environments where security outweighs unrestricted functionality. Suitability for typical managed environments depends on how tightly the hosts are managed and the extent of the risks that they face.[11]

The following are the AEC functions:

1. **Define and Maintain Application Execution Control Lists and Policies** captures the selection of applications on the Allow List and/or Deny List, and the associated policy in machine-readable form. Also provides for updates to the lists and policy.
2. **Control Installation/Execution** controls the installation and execution of software based on the agency defined AEC control policies. Allow List applications will be allowed to install and execute, while applications not on the list, and those appearing

[10] See current version of CDM LDM where devices of category "Endpoint" are defined.
[11] NIST SP 800-167

on the Deny List, will be subjected to blocking and other actions, based on agency policy.

3. **Provide Authorized User Interface** provides a user interface to conduct actions by an administrator.
4. **Exception Handling** provides administrators the ability to address AEC-detected issues. This function provides administrators the ability to respond to problems, by updating the Allow List or Deny List or the associated policy, providing temporary authorizations, or by taking some other agency approved action. This function could be pushed to first-line support, such as a help desk.
5. **Log Application Execution Control Events** logs attempts to install or execute an application not on the Allow List, or an application on the Deny List. It also has the ability to log successful attempts.
6. **Maintain and Report AEC Data** provides reports of interest, based on AEC logs, to assess events, when requested by an administrator and provides AEC data to the CDM dashboards. The CDM LDM provides guidance on the required data content. The complete details of the data set must be worked with the agency where policy decision and/or enforcement points are concerned.

Figure 4 presents a block diagram showing the relationship among AEC functions.

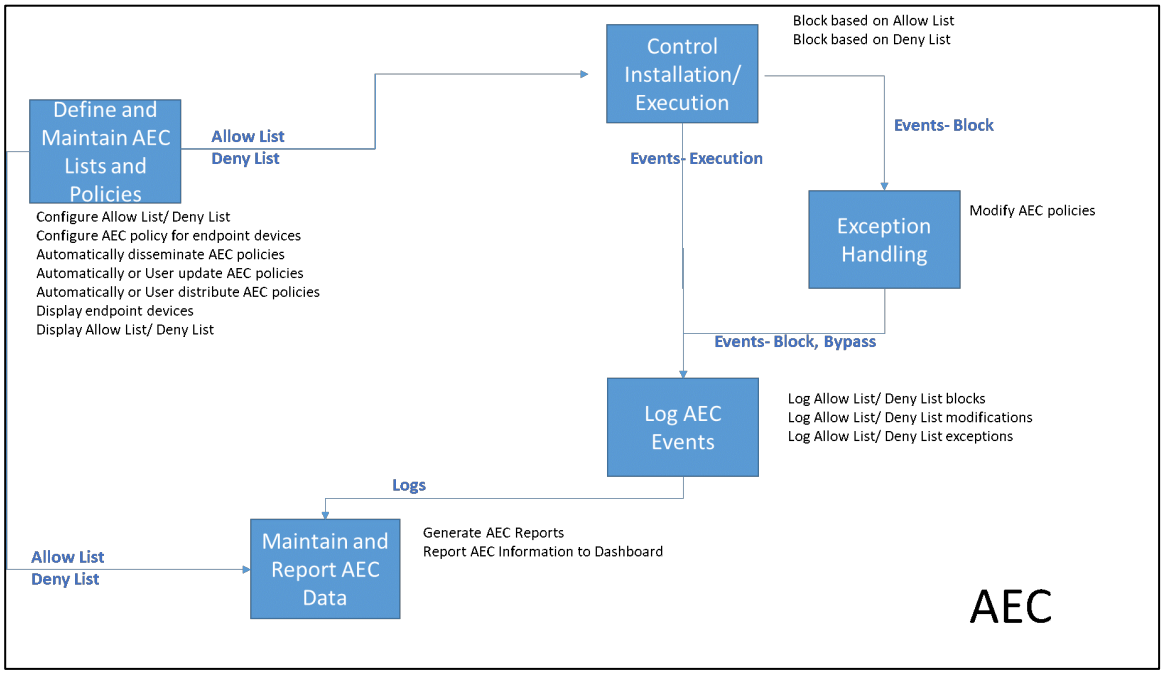

Figure 4. Workflow of Key AEC Functions

The following is a non-exclusive list of tool functionalities that support the AEC capability:

Tool Category Names	Summary of Functionality
Allow Lists and Deny List tools	Maintain and enforce software allow and deny lists
Software version scanning tools	Scanners send packets and read responses to discover hosts and services across the network, also to include version detection
Software deployment tools	Used to deploy or remove software
License management tools	Tracks software usage and for audit purposes, primarily to make sure the company is using the licenses they've purchased from different software vendors

2.2.2.1.1.1 CDM AEC Functional Requirements

This section provides functional requirements for the AEC capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 5 CDM AEC Functional Requirements

Summary	Description
Define and Maintain Execution Control List and Policies	
AEC-1-1	When configured by the administrator based on agency policy, the AEC capability shall instantiate the Allow List such that it incorporates between 95% (threshold) and 99% (objective) of the allowed applications on endpoint devices.
	Guidance: This is to develop or modify the applications on the Allow List and is desired state information used by the PEP.
AEC-1-2	When configured by the administrator based on agency policy, the AEC capability shall instantiate the Deny List such that it incorporates between 95% (threshold) and 99% (objective) of the denied applications on endpoint devices.
	Guidance: This is to develop or modify the applications on the Deny List and is desired state information used by the PEP.
AEC-1-3	If applicable, based on agency policy, the AEC capability shall implement different AEC control policies for each endpoint device type.
	Guidance: Devices that have a category of "Endpoint" to which this requirement applies include the following device types: workstations, laptops, thin clients, virtual desktops, and servers (all types).[12] Each endpoint device or device type may be configured differently, based on agency policy. The policy includes details on actions to be taken (log the attempt, notify the user, block the installation, etc.) when an unauthorized software (not on the Allow List or on the Deny List) installation or execution occurs.
AEC-1-4	When configured by the administrator based on agency policy, the AEC capability shall group endpoint devices together for implementation of configured allow and/or deny lists.
AEC-1-5	The AEC capability shall automatically disseminate control policies to attached endpoint devices upon administrator configuration change within 24 hours.
	Guidance: AEC control policies are defined to specify what actions are taken (log the attempt, notify the user, block the installation, etc.) when an attempt is made to install or execute an application not meeting the agency policy requirements.
AEC-1-6	The AEC capability shall automatically disseminate control policies to endpoint devices that were not connected to the network during an automatic update, upon connection to the network.
	Guidance: AEC control policies are defined to specify what actions are taken (log the attempt, notify the user, block the installation, etc.) when an attempt is made to install or execute an application not meeting the agency policy requirements.
AEC-1-7	When configured by the administrator based on agency policy, the AEC capability shall automatically update the Allow List on the intended execution date/time or on reception date/time of the update, whichever is later.
	Guidance: Some tools receive updates through automated feeds, such as Microsoft updates, making automatic updates possible. The intended execution date/time is included in the update and is the intended date/time for the update to be installed. Reception date/time is the date/time when the update is received. The intended execution date/time could be before or after the reception date/time, therefore, the requirement is based on whichever is later. This is the centrally managed Allow List. The intent is for Allow List updates to be timely enough for the PEP function invoked in AEC-2-1 to be effective against the threat (i.e., cyber relevant time).

[12] CDM Data Model Document, Version 3.8.1, March 2020

Summary	Description
AEC-1-8	The AEC capability shall automatically distribute application updates to agents on endpoint devices enforcing the Allow List within 24 hours of the intended execution date/time or reception date/time of the update, whichever is later, based on agency policy.
	Guidance: Some tools receive routine updates through automated feeds, such as Microsoft updates, making automatic updates possible. The intended execution date/time is included in the update and is the intended date for the update to be installed, it could be based on explicit input from the administrator or provided from external sources (e.g., provided by AEC tool vendor as informed by threat feeds). Reception date/time is the date/time when the update is received. The intended execution date/time could be before or after the reception date/time, therefore, the requirement is based on whichever is later. This is the distribution of the Allow List to the agents on endpoint devices.
AEC-1-9	For automated updates requiring administrator approval based on agency policy, the AEC capability shall automatically update the Allow List within upon the administrator's approval of the update.
	Guidance: Agencies may need to review automatic updates prior to deploying to endpoint devices. This is the centrally managed Allow List. The intent is for Allow List updates to be timely enough for the PEP function invoked in AEC-2-1 to be effective against the threat (i.e., cyber relevant time).
AEC-1-10	For automated updates requiring administrator approval based on agency policy, the AEC capability shall distribute the Allow List to agents on endpoint devices within 24 hours of the administrator's approval of the update.
	Guidance: Agencies should not distribute Allow List to agents on the endpoint devices before being reviewed and approved by the administrator. This is the distribution of the Allow List to the agents on endpoint devices.
AEC-1-11	When configured by the administrator based on agency policy, the AEC capability shall automatically update the Deny List on the intended execution date/time or reception data/time of the update, whichever is later.
	Guidance: Some tools will receive feeds containing emergent threat intelligence or vendor advisories and use this to automatically update the Deny List. The intended execution date/time is included in the update and is the intended date/time for the update to be installed. Reception date/time is the date/time when the update is received. The intended execution date/time could be before or after the reception date/time, therefore, the requirement is based on whichever is later. This is the centrally managed Deny List. The intent is for Deny List updates to be timely enough for the PEP function invoked in AEC-2-4 to be effective against the threat (i.e., cyber relevant time).
AEC-1-12	The AEC capability shall automatically distribute application updates to agents on endpoint devices enforcing the Deny List within 24 hours of the intended execution date/time or reception date/time of the update, whichever is later, based on agency policy.
	Guidance: Some tools will receive feeds containing emergent threat intelligence or vendor advisories and use this to automatically update the Deny List. Reception date/time is the date/time if/when the update is received by the AEC console/central server. The intended execution date/time could be before or after the reception date/time, therefore, the requirement is based on whichever is later. This is the distribution of the Deny List to the agents on endpoint devices.
AEC-1-13	For automated updates requiring administrator approval based on agency policy, the AEC capability shall automatically update the Deny List upon the administrator's approval of the update.
	Guidance: Agencies may need to review automatic updates prior to deploying to endpoint devices. This is the centrally managed Deny List. The intent is for Deny List updates to be timely enough for the PEP function invoked in AEC-2-4 to be effective against the threat (i.e., cyber relevant time).

Summary	Description
AEC-1-14	For automated updates requiring administrator approval based on agency policy, the AEC capability shall distribute the Deny List to agents within 24 hours of the administrator's approval of the update
	Guidance: Agencies should not distribute the Deny List before being reviewed and approved by the administrator. This is the distribution of the centrally managed Deny List to the agents on endpoint devices.
Control Installation/Execution	
AEC-2-1	Upon attempted installation or execution of an application that does not appear on the agency Allow List, the AEC capability shall block the requested action in cyber-relevant time, based on agency policy for the endpoint device.
	Guidance: This is a PEP function. Blocking of the application should be immediate, or near immediate.
AEC-2-2	The AEC capability shall have an average false negative (allow) rate of no greater than 0.1% of total Allow List application execution or installation attempts over a 30-day period, based on agency policy.
	Guidance: A false negative (allow) results when an application that is NOT on the Allow List is allowed to be installed or executed. The false negative (allow) rate is calculated by # of applications not on the Allow List allowed to install or execute divided by the total number of attempts to install or execute applications not on the Allow List.
AEC-2-3	The AEC capability shall have an average false positive (allow) rate of no greater than 0.1% of total Allow List application execution or installation attempts over a 30-day period, based on agency policy.
	Guidance: A false positive allow results when an application that is on the Allow List is NOT allowed to be installed or executed. The false positive Allow List rate is calculated by # of applications on the Allow List not allowed to install or execute divided by the total number attempts to install or execute applications on the Allow List.
AEC-2-4	Upon attempted installation or execution of an application that appears on the agency Deny List, the AEC capability shall block the requested action in cyber relevant time, based on agency policy for the endpoint device.
	Guidance: This is a PEP. Blocking of the application shall be in cyber relevant time.
AEC-2-5	The AEC capability shall have an average false positive (deny) rate of no greater than 0.1% of total Deny List application installation or execution attempts over a 30-day period, based on agency policy.
	Guidance: A false positive deny results when an application that is NOT on the Deny List is NOT allowed to be installed or executed. The false positive (deny) rate is calculated by # of applications not on the Deny List not allowed to install or execute divided by the total number attempts to install or execute applications not on the Deny List.
AEC-2-6	The AEC capability shall have an average false negative (deny) rate of no greater than 0.1% of total Deny List application installation or execution attempts over a 30-day period, based on agency policy.
	Guidance: A false negative (deny) results when an application that is on the Deny List is allowed to be installed or executed. The false negative (deny) rate is calculated by # of applications on the Deny List allowed to install or execute divided by the total number attempts to install or execute applications on the Deny List.
AEC-2-7	The AEC capability shall quarantine or remove all temporary and application-associated files while blocking the installation of an application, based on agency policy.
	Guidance: Applications may temporarily download files during the installation process and they will need to be removed or quarantined if the application is blocked.
AEC-2-8	The AEC capability shall enforce between 95% (T) and 99% (O) of the applications that are designated to be allowed on the Agency's desired state policy.
	Guidance: This requirement will be tested by dividing the number of applications designated as "allowed" (i.e., approved) in the AEC capability by the total number of applications in the Agency's desired state policy regarding "allowed" (i.e., approved) applications. Note that this is a per application count rather than per installation count. The use of the term 'enforce' relates to the intent to permit only those applications designated on the allow list to execute.

Summary	Description
AEC-2-9	The AEC capability shall block between 95% (T) and 99% (O) of the applications that are designated to be denied on the Agency's desired state policy
	Guidance: This requirement will be tested by dividing the number of applications designated as "denied" (i.e., prohibited) in the AEC capability by the total number of applications in the Agency's desired state policy regarding "denied" (i.e., prohibited) applications. Note that this is a per application count rather than per installation count.
Provide Authorized User Interface	
AEC-3-1	The AEC capability shall enforce role-based access control, based on agency policy.
	Guidance: The AEC capability may, at the discretion of the agency, integrate with implemented identity and access management capabilities, which may broker appropriate access based upon the policies deployed in the IdAM-related tools.
AEC-3-2	Upon administrator input, the AEC capability shall display the endpoint devices under control of the AEC capability, filtered and sorted based upon the administrator's selection.
	Guidance: Filtering and sorting examples for consideration include device properties (e.g., IP address, hostname, etc.).
AEC-3-3	Upon administrator input, the AEC capability shall display the Allow List applications, filtered and sorted based on the administrator's selection.
	Guidance: Filtering and sorting examples for consideration include device properties (e.g., IP address, hostname, etc.) or application identifying information (Application name, category, etc.).
AEC-3-4	Upon administrator input, the AEC capability shall display the Deny List applications, filtered and sorted based upon the administrator's selection.
	Guidance: Filtering and sorting examples for consideration include device properties (e.g., IP address, hostname, etc.) or application identifying information (Application name, category, etc.).
AEC-3-5	Upon administrator input, the AEC capability shall display the blocked applications, filtered and sorted based upon the administrator's selection.
	Guidance: The administrator can obtain a filtered view of blocked applications upon input. Blocked applications are applications that were attempted to be installed or executed but were blocked by the AEC capability.
AEC-3-6	Upon administrator input, the AEC capability shall generate customized reports, based on Agency policy.
	Guidance: The administrator must be able to select the custom AEC capability data to be contained in the report.
AEC-3-7	When configured by the administrator based on agency policy, the AEC capability shall generate predefined reports on a scheduled basis.
	Guidance: Some reports may be predefined by the AEC capability tools; others may be customized by the administrator to support specific Agency operational reporting needs.
AEC-3-8	When configured by the administrator based on agency policy, the AEC capability shall e-mail reports to a distribution list defined by the administrator.
Exception Handling	
AEC-4-1	Upon administrator input, the AEC capability shall modify the Allow List upon user request to enable execution of blocked applications.
	Guidance: Authorized users such as administrators may make exceptions to AEC policies upon user request with adequate business justification to allow applications to be placed on the Allow List (see AEC-4-2), grant a user privilege to install an application, etc.
AEC-4-2	Upon administrator input, the AEC capability shall modify the Deny List upon user request to enable execution of blocked applications.
	Guidance: Authorized users such as administrators may make exceptions to AEC policies upon user request with adequate business justification to allow installation of applications on the Deny List (see AEC-4-2), grant a user privilege to install an application, etc.
Log Application Execution Control Events	
AEC-5-1	The AEC capability shall log user, device, and application information related to each attempt to install or execute applications that are not on the agency's Allow List.

Summary	Description
	Guidance: Logging of details may include: user ID, device, IP address, time, or type/name of application attempted.
AEC-5-2	The AEC capability shall log user, device, and application information related each attempt to install or execute applications that are on the agency's Deny List.
	Guidance: Logging of details may include: user ID, device, IP address, time, or type/name of application attempted.
AEC-5-3	The AEC capability shall log each modification to agency's Allow List by administrators.
	Guidance: Logging of details may include: user, device, IP address, time, or application.
AEC-5-4	The AEC capability shall log each exception to agency's existing Allow List for selected users.
	Guidance: Logging of details may include: user, device, IP address, time, or application. See requirements AEC-4-1 and AEC 4-2 to which this requirement relates.
AEC-5-5	The AEC capability shall log each modification to agency's Deny List by administrators.
	Guidance: Logging of details may include: user, device, IP address, time, or application.
AEC-5-6	The AEC capability shall log each exception to agency's existing Deny List for selected users.
	Guidance: Logging of details may include: user, device, IP address, time, or application.
AEC-5-7	The AEC capability shall log each attempt to install or execute an application.
	Guidance: This information is needed for test purposes to calculate the performance in AEC-2-3, and AEC-2-5. The log can be used to identify the total number of attempted installations/executions of applications on the allow list and also not on the deny list.
AEC-5-8	The AEC capability shall automatically export AEC capability event data to external log and event management solutions, based on agency policy.
	Guidance: This requirement is intended to be refined during solution engineering and integration, based on agency policy.
Maintain and Report AEC Data	
AEC-6-1	The AEC capability shall continuously maintain a timely, updated inventory of blocked applications on the Agency network, including blocked-application meta-data.
AEC-6-2	The AEC capability shall report a collection of AEC data that includes the following about unauthorized applications: • Attempts to execute unauthorized software • Software authorization status • Device meta-data, such as the hostname and IP address of the device • Software meta-data, such as the version, vendor, and product name and/or executable name of the unauthorized application • Timestamp of last software inventory update
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts. See LDM for definitions of UnauthorizedSWEventOnNetwork.

2.2.3 Security Configuration Settings Management (CSM) Capability

The security CSM capability reduces misconfiguration of assets, including misconfigurations of devices (physical and virtual machines), as well as associated operating systems (OSs) and critical software. Cyber adversaries often use automated scanning attacks to search for and exploit assets with misconfigurations, and then pivot to attack other assets.[13,14]

The CSM capability interrogates targeted devices for compliance against security configuration benchmarks (CSM benchmarks[15]). A CSM benchmark is a checklist that is used through one or more CDM tools to automatically and continuously verify configuration settings of a given device based on the contents of the checklist. A security configuration benchmark contains instructions or procedures for configuring an IT product to an operational environment, for verifying that the product has been configured properly, and/or for

[13] See https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical- cyber-threat-framework.pdf. Note the section on LATERAL MOVEMENT.
[14] See https://attack.mitre.org/tactics/TA0008/.
[15] Refer to the Program's Data Dictionary (AV-2) for the formal definition of a security configuration benchmark.

identifying unauthorized configuration changes to the product. Automated checklists document their security settings in a machine-readable format. The CDM program's standard for the CSM capability is the Security Content Automation Protocol (SCAP).

Security configuration benchmarks may be modified, or tailored, by Agencies as approved deviations from the original content; however, certain conditions apply to their impact on reporting within the CDM solution.[16] Either in original or modified form, such benchmarks may be representative of an Agency's desired state for CSM. CSM benchmarks may be grouped into a "benchmark grouping", which is a collection of CSM benchmarks and customizations used to evaluate CSM-related configuration items on a device at scan time. For example, the OS benchmark and software application benchmark(s) could be grouped to apply to a typical Agency endpoint.

CSM benchmarks specify desired value(s) (i.e., desired state) for each relevant security configuration setting for the device category and type being targeted. Differences between desired and actual security configuration settings represent a change in risk to the system. This difference may make the information system less secure or more secure, which may be accounted for in the risk score determination.[17]

The CSM capability leverages the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)[18] as the de-facto standard for identifying configuration settings that impact a system's overall risk posture. STIG CAT I findings are used in the current (v1.x) Agency-Wide Adaptive Risk Enumeration (AWARE) scoring algorithm. STIG CAT I configuration items represent key settings on software (inclusive of OS) where deviation from the desired state present severe, potentially exploitative, conditions that can directly result in a loss of confidentiality, availability, or integrity.

CSM also supports the management of security configuration settings associated with the specialized capabilities needed for processing or storing of sensitive information such as personally identifiable information (PII).

The following are the security CSM functions (applicable requirements are shown in parentheses):

1. **Manage Benchmarks** manages all aspects of CDM CSM benchmarks including desired state benchmarks, customized benchmarks, access control of benchmarks, maintaining currency of benchmarks, tracking changes, and displaying customized benchmarks. (CSM-1-1 through 1-5, CSM-3-1 through 3; CSM-4-1, CSM-4-3)
2. **Manage Benchmark Groupings** manages aspects of groupings of CDM CSM benchmarks including managing grouping identifiers, tracking changes, and limiting access to benchmark groupings. (CSM-4-2, CSM-4-4, CSM-6-3 through 6-5)
3. **Group Devices and Assign Benchmarks** organizes devices and assigns devices to benchmark groupings. (CSM-5, CSM-6-1, CSM-6-2)
4. **Compare Actual Configuration Settings to Benchmarks** identifies differences between the actual state and the desired state of configuration settings and maintains an inventory of configuration settings. (CSM-2-1 through 2-3, CSM-7, CSM-9-1)
5. **Report CSM Inventory of Security Configuration Settings** reports the inventory of security configuration settings for devices scanned. (CSM-8)

[16] See Configurations Settings Management Guidance, Version 1, January 2021, for a broader discussion of CSM tailoring.
[17] See Continuous Diagnostics and Mitigation (CDM) Agency-Wide Adaptive Risk Enumeration (AWARE) Technical Design Document, Version 1.2, 16 October 2019.
[18] https://nvd.nist.gov/ncp/repository (Select: "Defense Information Systems Agency" under "Authority.")

The following is a non-exclusive list of general tool functionalities (i.e., tool categories that provide CSM functional requirements):

Tool Category Name	Summary of Functionality
Unified Endpoint Management Tools	Configure endpoint devices; determine device compliance
Endpoint/Network Device Management Tools	Configure and manage network devices
SCAP configuration assessment tools	Identify differences from the desired security configuration settings that have published SCAP content
Benchmark management tools	Manage benchmarks Maintain Inventory of Configuration Settings for Devices

The following is a non-exclusive list of tools that CSM may integrate with:

Tool Category Name	Summary of Functionality
Asset Management Tools	Reduce misconfiguration of assets by comparing desired states with actual states
SIEM Tools	Logging of CSM administrator actions and CSM management

2.2.3.1 CSM Functional Requirements

This section provides functional requirements for the CSM capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine-readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 6. CSM Functional Requirements

Req. UID	Requirement Text
CSM-1-1	When input by the administrator, the CSM capability shall store CSM benchmarks for use in scanning installed software on target devices for defects.[19]
	Guidance: Installed software also includes OSs that are installed on the targeted device.
CSM-1-2	The CSM capability shall maintain a UID for each stored CSM benchmark used to scan devices on the network.
	Guidance: This functionality allows for unique identification of different benchmarks (e.g., benchmark name, version, etc.) used to scan devices on the network for defects.
CSM-1-3	The CSM capability shall maintain customizations to CSM benchmarks, as input by the administrator.
	Guidance: "Customize"/ "Customization" is also referred to as "tailoring" which is a process to adapt, traditionally, well-known, standard configuration benchmarks (i.e., STIGs, CIS, etc.) for use within an agency's environment (i.e., defining a custom "desired state" based on agency policy). "Maintain"/ "Maintenance" includes the creation, updating/replacement, or deletion of security configuration settings benchmarks, their customizations, or their exceptions.
CSM-1-4	The CSM capability shall track any customizations made to stored CSM benchmarks.
	Guidance: "Customize"/"Customization" is also referred to as "tailoring" which is a process to adapt, traditionally, well-known, standard configuration benchmarks (i.e., STIGs, CIS, etc.) for use within an agency's environment (i.e., defining a custom "desired state" based on agency policy). "Track"/ "Tracking" refers to a function that records or otherwise notes (i.e., "track") the relevant details (i.e., who / what action) regarding some interaction between a user/administrator and the capability such that subsequent logging or displaying of the interaction can be executed.
CSM-1-5	The CSM capability shall display customizations made to stored CSM benchmarks by date and by administrator who made the change.

[19] Refer to the Program Data Dictionary (AV-2) for the formal definition of *Defect*.

Req. UID	Requirement Text
CSM-2-1	Upon administrator input, the CSM capability shall execute an ad-hoc scan on target devices to identify any differences between the actual detected configuration settings when compared against CSM benchmark(s) used for that target device.
	Guidance: Multiple benchmarks could be used for a single device depending on the scope of the scan as defined by the administrator (applications, OS, etc.) of a device. This includes differences that provide greater protection or reduce risk further than the CSM benchmark.
CSM-2-2	When configured by the administrator, the CSM capability shall automatically scan target devices to identify any differences between the actual detected configuration settings when compared against CSM benchmark(s) based a trigger event or defined schedule.
	Guidance: Multiple benchmarks could be used for a single device depending on the scope of the scan as defined by the administrator (applications, OS, etc.) of a device. This includes differences that provide greater protection or reduce risk further than the CSM benchmark. Agency policies dictate what the configuration settings are for the CSM benchmark(s) (i.e., desired state) for any device category or platform that is not covered by the program's requirements (i.e., CSM-9-1).
CSM-2-3	When configured by the administrator, the CSM capability shall authenticate to devices to conduct a scan.
	Guidance: Acceptable authentication methods are defined by the Agency. In the future CDM may specify more explicit Common requirements regarding PIV or SSO support, to align with Federal mandates.
CSM-3-1	The CSM capability shall log when any of the following occur: • New CSM benchmarks are created (i.e., stored) • Existing CSM benchmarks are updated/replaced • Existing CSM benchmarks are deleted/removed
CSM-3-2	The CSM capability shall log all administrative actions taken on Agency exceptions to CSM benchmarks.
	Guidance: "Administrative actions" include any activity that is associated with creating, updating, and/or deleting stored CSM benchmarks, their customizations, and/or their exceptions.
CSM-3-3	The CSM capability shall log all administrative actions taken on Agency customizations to CSM benchmarks.
	Guidance: "Administrative actions" include any activity that is associated with creating, updating, and/or deleting stored CSM benchmarks, their customizations, and/or their exceptions.
CSM-4-1	The CSM capability shall enforce access control such that maintenance of stored CSM benchmarks, including their customizations and their exceptions, are only performed by the administrator.
	Guidance: "Maintain"/ "Maintenance" includes the creation, updating/replacement, or deletion of security configuration settings benchmarks, their customizations, or their exceptions.
CSM-4-2	The CSM capability shall enforce access control such that maintenance of CSM benchmark groupings are only performed by the administrator.
	Guidance: "Maintain"/ "Maintenance" includes the updating/replacement or deletion of security configuration settings benchmarks, their customizations, or their exceptions. "CSM benchmark grouping" is a collection of CSM benchmarks and customizations, which evaluate CSM-related configuration items on the device at scan time, which directly support an at large security configuration for a device.
CSM-4-3	The CSM capability shall authorize maintenance of stored CSM benchmarks, including their customizations and their exceptions, are granted on a per CSM Benchmark basis.
	Guidance: "Maintain"/ "Maintenance" includes the creation, updating/replacement, or deletion of security configuration settings benchmarks, their customizations, or their exceptions.
CSM-4-4	The CSM capability shall restrict which administrators can modify CSM benchmark groupings on a security benchmark grouping basis, based on agency policy.

Req. UID	Requirement Text
	Guidance: "CSM benchmark grouping" is a collection of CSM benchmarks and customizations, which evaluate CSM-related configuration items on the device at scan time, which directly support an at large security configuration for a device.
CSM-5	When configured by the administrator, the CSM capability shall group devices together for assigning CSM benchmarks to those devices for scanning.
CSM-6-1	When configured by the administrator, the CSM capability shall group multiple CSM benchmarks together to establish an Agency-defined grouping of CSM benchmarks for devices.
	Guidance: An asset may have multiple installed items (firmware, OS, applications) that require multiple configuration settings benchmarks (and their associated configuration checks). This requirement allows grouping of those individual benchmarks to support a security configuration for the device. A benchmark grouping may consist of multiple CSM benchmarks (OS and software application benchmarks), as determined by agency policy (e.g., SSPs) and the associated configuration management process at the agency.
CSM-6-2	When configured by the administrator, a CSM benchmark grouping assigned to devices shall also assign the grouping's associated CSM benchmarks to the devices for scanning.
	Guidance: "CSM benchmark grouping" is a collection of CSM benchmarks and customizations, which evaluate CSM -related configuration items on the device at scan time, which directly support an at large security configuration for a device.
CSM-6-3	The CSM capability shall maintain a UID for each CSM benchmark grouping on the network.
	Guidance: "CSM benchmark grouping" is a collection of CSM benchmarks and customizations, which evaluate CSM-related configuration items on the device at scan time, which directly support an at large security configuration for a device.
CSM-6-4	The CSM capability shall track changes made to any CSM benchmark grouping
	Guidance: "CSM benchmark grouping" is a collection of CSM benchmarks and customizations, which evaluate CSM-related configuration items on the device at scan time, which directly support an at large security configuration for a device.
CSM-6-5	The CSM capability shall display changes in CSM benchmark groupings by date and by administrator who made the change
	Guidance: "CSM benchmark grouping" is a collection of CSM benchmarks and customizations, which evaluate CSM-related configuration items on the device at scan time, which directly support an at large security configuration for a device
CSM-7	The CSM capability shall maintain a timely, updated CSM inventory of security configuration settings for devices on the Agency network, including configuration benchmark used, applicable documented exception, discovery date, remediation/fix description, desired state value and actual state observed.
CSM-8	The CSM capability shall report the CSM inventory of security configuration settings for devices scanned on the Agency network, including configuration benchmark used, applicable documented exception, discovery date, remediation/fix description, desired state value and actual state observed.
	Guidance: This requirement supports CSM inventories which are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards). This includes STIG CAT I findings which are utilized in the AWARE scoring algorithm. This requirement should be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents).
CSM-9-1	When configured by the administrator, the CSM capability shall scan installed operating system(s) on endpoint devices to identify any differences from the DISA STIG CAT 1 security configuration settings that have published SCAP content.

Req. UID	Requirement Text
	Guidance: See the site: https://public.cyber.mil/stigs/ for the applicable software on endpoint devices that are in scope of the STIGs and this requirement. Note that this requirement includes only OSs resident on any endpoint device for which there is an associated STIG benchmark which has CAT 1 settings. Refer to the program data dictionary (AV-2) for the definition of endpoint device. SCAP content refers to the machine-readable policy content (typically XML based-Extensible Configuration Checklist Description Format [XCCDF]) that is published for CSM tool use in order to automate CSM defect checks, furnished by DISA and/or through the national checklist repository: https://nvd.nist.gov/ncp/repository

2.2.4 Vulnerability Management (VUL) Capability

The CDM VUL capability detects known software vulnerabilities, including for example, authentication errors, path errors, and buffer overflows, on assets on the network. These vulnerabilities are mistakes or deficiencies in software that an adversary could use to gain access to a system or network and thereby be able to pivot to obtain unauthorized access to sensitive data. The detection and reporting of these vulnerabilities help enable remediation or mitigation by the consumers of the information (security operation personnel).

The VUL capability detects and reports industry-codified [i.e., traceable to the National Vulnerability Database (NVD[20])] software vulnerability risk indicators to the CDM Agency Dashboard. This is to support the implementation of the Agency Wide Adaptive Risk Enumeration (AWARE) algorithm, the standardized metrics employed in the Ongoing Assessment functionality, and to populate general cyber relevant reports intended for senior stakeholder decision-making related to vulnerability management.

Within Layer A of the CDM architecture (tools and sensors), the VUL capability detects vulnerabilities in assets on the network. Within the B layer of the CDM architecture, vulnerabilities are correlated with other datasets to form CDM records (also referred to as CDM objects), including the Master Device Record (MDR), and reports them to the CDM Dashboards. The VUL capability enables improved vulnerability management for participating Agencies through this correlation with other cyber relevant data. HWAM (catalogs hardware), SWAM (documents software), and CSM (documents configuration settings) provide information to VUL. There may be multiple sensors implementing the VUL capability, if necessary, to maximize vulnerability detection and reporting.

The VUL capability integrates with the NVD to detect and report vulnerabilities as Common Vulnerabilities and Exposures (CVEs). The VUL capability may also identify other detectable vulnerabilities that have available remedies not in the NVD.

The VUL capability functions and associated goals are:

- **Keep vulnerability database current**
  - Continuously update vulnerability signatures
  - Customize vulnerability signatures, based on Agency operational needs and policy
- **Detect vulnerabilities**
  - Timely detection of new CVEs
  - Reflect remediation and patching efforts by the Agency
  - Maximize vulnerability detection above the minimum operational thresholds of the CDM Program
  - Minimize false-negative scenarios (e.g., non-reporting, non-detection of real vulnerabilities through improper configuration of the VUL tools and sensors or network infrastructure)
  - Minimize false-positive scenarios (e.g., maximizing timely and accurate detection and reporting of vulnerabilities as they are remediated by the Agency)

[20] See https://nvd.nist.gov/ for further information.

- **Log and alert on VUL events**
  - VUL events could include, for example, vulnerability scan start, stop, and error conditions such as failed authentication by the scanner, as well as privileged configuration changes of the scan policies, or equivalent, themselves.
- **Provide Authorized User Interface**
  - Conduct actions by an authorized user or role
- **Maintain and report CDM data**
  - Furnish quality vulnerability data, fit for use to the Agency Dashboard to support its key functions (e.g., AWARE, Ongoing Assessment functions, etc.)

Vulnerabilities detected will typically be remediated through separate software inventory management functions, using updates, patches, plug-ins, and new releases.

Detection and reporting of Common Weakness Enumeration (CWE) data is aligned with the CDM DBS capability. However, CVE detection and reporting of any asset type or class aligns with the VUL capability.

The following is a non-exclusive list of tool functionalities that support the VUL functional requirements:

Tool Category Name	Summary of Functionality
Vulnerability scanners (network or agent based)	Assists security administrators to detect system weaknesses across the network, classify vulnerabilities, and implement countermeasures

2.2.4.1 VUL Functional Requirements

This section provides functional requirements for the VUL capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine-readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 7. VUL Functional Requirements

Req. UID	Requirement Text
Keep Vulnerability Database Current	
VUL-1-1	The VUL capability shall update vulnerability detection signatures in an automated manner at an interval of no greater than 24 hours from the last signature update.
	Guidance: The vulnerability database may also be updated based upon authorized user request per VUL-1-3.
VUL-1-2	The VUL capability shall apply Common Vulnerability Scoring Standard (CVSS) v2 and CVSS v3 scores from the NVD to the vulnerabilities.
	Guidance: Some older vulnerabilities use CVSS v2 while newer ones use v3. Support for both standards is therefore expected.
VUL-1-3	Upon administrator input, the VUL capability shall download and apply vulnerability signature detection updates to its vulnerability database.
	Guidance: This provides for an immediate update outside of the automatic update period. The vulnerability database is the list of CVEs from the NVD that are supported and testable within the VUL capability.
VUL-1-4	When configured by the administrator, the VUL capability shall customize vulnerability detection signatures.
	Guidance: This allows an administrator to modify or create custom vulnerability detection signatures because some vulnerabilities might not be available in the public repository or to allow customization based on Agency policy. The intent for this requirement is not to customize the vulnerability metadata.

Req. UID	Requirement Text
Detect Vulnerabilities	
VUL-2-1	When configured by the administrator, the VUL capability shall scan devices on the network to detect software vulnerabilities on an automated basis with an average (over a 30 day period of all scans conducted) false positive rate of no greater than 0.1%.
	Guidance: A false-positive for the VUL capability is defined as any scenario where a vulnerability is detected/reported on a device when it is confirmed not to exist, some specific examples include: (i) duplicate vulnerability reporting relative to a given device, (ii) reporting vulnerabilities in the CDM solution which have been confirmed to be remediated, (iii) an improperly configured VUL sensor that falsely detects a non-existent vulnerability. The false positive rate is calculated by # of vulnerabilities detected that are confirmed to not exist on the device divided by the total # of detected vulnerabilities for that device.
VUL-2-2	When configured by the administrator, the VUL capability shall implement non-disruptive scans on specific devices to detect vulnerabilities.
	Guidance: VUL must be capable of employing non-disruptive and non-destructive scanning methods and configurations so resident business functions may continue to support Agency operations.
VUL-2-3	When configured by the administrator, the VUL capability shall authenticate to devices to conduct a scan.
	Guidance: *(1) This applies regardless of whether network-based or agent-based vulnerability identification is used.* *(2) Proper system and network configuration require a partnership with agency IT management stakeholders.* *(3) The intent of this requirement is to help minimize false-negative vulnerability detection and thereby mischaracterizing Agency AWARE scores and other reports at the CDM Dashboard. See VUL-2-4, which relates to this requirement.* *(4) Device types that do not support direct VUL capability authentication may be reported to CDM Portfolio teams for resolution on a case by case basis in accordance with current Program guidance.* *(5) Acceptable authentication methods are defined by the Agency. In the future CDM may specify more explicit Common requirements regarding PIV or SSO support, to align with Federal mandates.*
VUL-2-4	When configured by the administrator, the VUL capability shall have privileged access to devices when conducting a scan.
	Guidance: *(1) The intent of this requirement is to help ensure the VUL capability achieves maximum vulnerability detection when interacting with scanned devices. See VUL-2-3, which relates to this requirement.* *(2) Device types that do not support direct privileged VUL capability interaction may be reported to CDM Portfolio teams for resolution on a case by case basis in accordance with current Program guidance.*
VUL-2-5	When configured by the administrator, the VUL capability shall integrate with the Agency privileged access management solution to allow for secure centralized privileged access on the scanned device, based on Agency policy.
	Guidance: See VUL-2-4. The intent of this requirement is to enable increased secure centralized privileged access management for the Agency through its integration with the VUL capability. This integration is intended generally and not intended to exclusively relate to the CDM Identity and Access Management capability.
VUL-2-6	When configured by the administrator, the VUL capability shall detect software vulnerabilities on an automated basis with an average (over a 30-day period of all scans conducted) false negative rate of no greater than 0.1%.

Req. UID	Requirement Text
	Guidance: See VUL-2-3, which will contribute to this requirement's satisfaction. A false-negative for the VUL capability is defined as any scenario where a vulnerability is confirmed to exist on a device, but is not detected/reported by the VUL capability, some specific examples include: (1) improperly configured VUL sensor that is not configured to detect all possible vulnerabilities of a given device (e.g., missing or disabled plug-ins/signatures) and/or (2) the VUL sensor is restricted in interrogating the device for vulnerabilities due to network restrictions such as firewalls or lack of privileges on the device.
VUL-2-7	The VUL capability database shall cover all NVD CVEs that are, at minimum, within 10 years of the original CVE publication date that are applicable to all scanned devices on the network.
	Guidance: This requirement is to be verified by analysis, by comparing (1) the NVD CVEs within 10 years of the original CVE publication date that are "applicable to network assets" (e.g., Windows assets would not be expected to be tested against Linux CVE) and (2) the VUL capability vulnerability database and to make sure all of the CVEs identified in (1) appear in the database. *The required temporal span of CVE coverage is established to ensure an operationally-relevant minimum of VUL detection and reporting breadth in relation to National Cyber Awareness System [21] alerting. Exceeding this span of coverage is not restricted and may be construed as the threshold.*
VUL-2-8	When executing a scan, the VUL capability shall detect between 80% (threshold) and 95% (objective) of vulnerabilities from the VUL capability database on all scanned devices on the network.
	Guidance: Detected vulnerabilities which are attributable to a CVE ID in the NVD should be used in verification of this requirement. – *This requirement traces to CDM ORD objectives, specifically to KPP1.3.* – *The intent is to ensure the VUL capability is configured to maximize detectable vulnerability coverage within the operational threshold and objective range.* – *Direct inspection and analysis of the VUL capability database (VUL-2-7) and sensor tool configuration identifies the set of CVEs that the VUL capability is configured to be able to detect. Inspection and analysis will assess the # of detectable vulnerabilities on all devices being scanned / number of known vulnerabilities on those devices published in the NVD within last 10 years such that greater than or equal to 80% of these known vulnerabilities will be detected.*
VUL-2-9	Upon administrator input, the VUL capability shall scan IP addressable devices on the network for software vulnerabilities.
	Guidance: This initiates an immediate scan outside of the periodically scheduled scans.
VUL-2-10	Upon administrator input, the VUL capability shall scan devices for specific vulnerabilities.
	Guidance: This initiates an immediate scan, but only for vulnerabilities specified by the administrator on all or select assets.
VUL-2-11	When configured by the administrator, the VUL capability shall detect those vulnerabilities that are remediated by the Agency.
	Guidance: The intent is for continuous refresh of the detected vulnerabilities to reflect Agency patching and/or remediation activity so that the user can obtain a current and accurate understanding of vulnerability exposure and attack surface. See VUL-4-6.
Log and Alert on VUL Events	
VUL-3-1	The VUL capability shall log event data associated with scanner authentication events against a target endpoint.
	Guidance: See VUL-2-3: logged data is expected to relate to this requirement.
VUL-3-2	The VUL capability shall log event data associated with enforcing access control to the VUL capability console, based on Agency policy.
VUL-3-3	The VUL capability shall log the event data associated with vulnerability signature updates.
	Guidance: See VUL-1-1: logged data is expected to relate to this requirement.

[21] See https://www.us-cert.gov/ncas/alerts.

Req. UID	Requirement Text
VUL-3-4	The VUL capability shall automatically export VUL capability event data to external log and event management solutions, based on agency policy.
	Guidance: This requirement is intended to be refined during solution engineering and integration, based on agency policy.
Provide Authorized User Interface	
VUL-4-1	The VUL capability shall enforce access control to authenticate selected roles to the console, based agency policy.
	Guidance: The vulnerability capability is expected to integrate with the identity and access management capability implemented by the agency, as based on Agency policy.
VUL-4-2	Upon input by the administrator, the VUL capability shall display the vulnerability database on the console.
	Guidance: The vulnerability database is the list of CVEs from the NVD that are supported and testable within the vulnerability capability. This functionality should allow the administrator to see what vulnerabilities are detectable by the VUL capability.
VUL-4-3	Upon input by the administrator, the VUL capability shall display the complete set of detected VUL capability data.
	Guidance: The identified VUL capability data is the set of data constructed by the vulnerability capability as a result of scans (i.e., detected vulnerabilities, findings, etc.).
VUL-4-4	Upon input by the administrator, the VUL capability shall display the identified VUL capability data for a single scan.
	Guidance: The administrator can select any scan saved in the historical data.
VUL-4-5	The VUL capability shall display a hyperlink to the National Vulnerability Database for each CVE in the displayed vulnerability data.
VUL-4-6	The VUL capability shall display the current status of the vulnerability in the displayed VUL capability data.
	Guidance: The current status could be remediated, open, etc.
VUL-4-7	When configured by the administrator, the VUL capability shall generate customized reports, based on Agency policy.
	Guidance: The administrator must be able to select the VUL capability data to be contained in the report.
VUL-4-8	Upon input by the administrator, the VUL capability shall generate reports filtered by an administrator-customized selection of criteria, based on Agency policy: • Device category, types • Subnet – Classless or Classful • CVSS based risk scores • Vulnerability status (remediated, open, etc.) • CVE ID
VUL-4-9	When configured by the administrator, the VUL capability shall generate predefined reports on a scheduled basis, based on Agency policy.
	Guidance: Some reports may be predefined by the VUL capability tools, others may be customized by the administrator.
VUL-4-10	When configured by the administrator, the VUL capability shall e-mail reports to a distribution list defined, based on agency policy.
Maintain and Report CDM Data	
VUL-5-1	The VUL capability shall continuously maintain a timely, updated inventory of detected vulnerabilities for devices on the Agency network, including vulnerability scanning metadata.

Req. UID	Requirement Text
VUL-5-2	The VUL capability shall report a collection of VUL data that includes the following information: • Device metadata: Hostname, OS, IP address • CVE ID • CVE dates originally discovered and remediated, if applicable • Authentication success or no • Vulnerability fix text
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical and physical data models, data requirement documents). Reported inventories are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards). *Examples of metadata may include at a minimum:* *– Unique vulnerability signature used to identify vulnerability* *– Time of scan execution start* *– Time of scan completion* *– Whether or not the scan identification successfully completed* *– Whether or not privileged authentication was used* *– CVE ID* *– Discovery and remediation dates* *– Vulnerability signature update events - timestamp, pass, fail* *– "Vulnerability Fix Text" – descriptive information that explains clearly and simply how to correct the vulnerability.*

2.2.5 Enterprise Mobility Management (EMM) Capability[22]

Enterprise Mobility Management (EMM) is a suite of services and technologies that enables an agency to secure the use of mobile devices (such as tablets, smartphones and E-readers), per the Agency's policies. The mobile device management component of the EMM enforces Agency security policies including the execution of the following actions on mobile devices:

- Installation and Management of Software
- Data Access Management
- Configuration Settings Management
- Device Compliance for Enterprise Access
- Monitoring and Tracking Equipment
- Device Locking/Wiping
- Access control to Sensors (for example camera, microphone)
- Cryptography and Encryption

The mobile application management component of the EMM provides the capability to manage software and services required for the provisioning and control of mobile applications, which are commercially available through public app stores or internally through an app catalog. Application management involves a wide range of capabilities, including:

- Deployment, updating, and removal of mobile apps
- Selectively wiping or encrypting app data
- Restricting the installations of specific apps through Allow Lists or Deny Lists
- Disabling access to public app stores and other carrier pre-installed apps

[22] NIST SP 800-124 Revision 2, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," 24 March 2020, and National Information Assurance Partnership, "Protection Profile for Mobile Device Fundamentals v3.1," 16 June 2017

- Integrating with Mobile App Vetting solutions to identify vulnerable or potentially malicious apps
- Restricting the permissions (for example, camera access, location access) assigned to each app
- Maintaining an inventory of apps on the mobile device

Application management will provide the information needed from a CDM perspective by providing an inventory of apps that are allowed (whitelisted) or disallowed (blacklisted), an inventory of applications that are installed to include known versions of applications that have vulnerabilities, and application policy settings. This information is needed to provide a view of the network health and can be tracked over time to determine whether network security is improving or getting worse.

The mobile identity management component of the EMM supports, depending on an Agency's policy, the issuance and life cycle management of credentials provisioned on mobile devices. EMM identity management may be tightly integrated with third-party vendor solutions for issuance and life cycle management of credentials, including non-person-entity (NPE) or device certificates, and the derived personal identity verification (PIV) credentials. This includes facilitating the revocation of the credentials when the devices are wiped or disabled. EMM identity management allows for integration with enterprise identity, credential, and access management (ICAM) solutions to ensure that only trusted apps on trusted devices are accessing enterprise data, particularly with cloud services. Features include blocking access to cloud services from apps and devices that are not authorized, integration with identity providers, and support for federated authentication. Authentication mechanisms include userid/password, biometrics (for example, fingerprint, iris scan), and certificate (PIV derived or other) to the device and apps. Access to apps and data may be controlled based on environmental attributes (for example, location, time of day) as well as end user attributes (for example, group membership).

In addition to mobile device, application, and identity management, EMM needs to integrate with Mobile Application Vetting (MAV) and Mobile Threat Defense (MTD) capabilities. MAV tools perform enterprise-level security analysis of managed apps and their libraries prior to deployment and throughout the lifecycle of the apps. MTD tools help detect the presence of malicious apps or software, malicious activity, and connections to blacklisted websites or networks. Integration of EMM with MAV provides the ability for MAV to update app reputation to allow the EMM to provide mitigations (for example, uninstall app, block access to enterprise resources) against apps with unacceptable reputation scores. Integration of EMM with MTD provides the ability of MTD to notify the EMM of malicious apps or activity on a mobile device to allow the EMM to provide mitigations (for example, uninstall app, block access to enterprise resources) for malicious apps or activity. Mobile device protection capability includes EMM integration with MAV and MTD.

The following is a non-exclusive list of tool functionalities that support the EMM functional requirements:

Tool Category Name	Summary of Functionality
Enterprise Mobility Management tools	Enables administrators to enforce required security measures, remotely configure applications, and securely grant access to data
Unified Endpoint Management tools	Manages all the endpoint devices within an organization from a central location, such as: security updates, patch management, HW and SW inventory tracking, logging, mobile device management, software and OS deployment, and workstation remote control
Asset management tools	IT asset management is a set of business processed designed to help IT departments track, control, and maintain the business's IT assets, including hardware and software.
Mobile Device Management tools	Secures employee personal mobile devices, protecting against malware, protecting data, and assists with set up of new devices
Mobile Application Management tools	Enables the license management, distribution, securing, and life cycle management of apps for mobile devices

2.2.5.1 EMM Functional Requirements

This section provides functional requirements for the EMM capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine-readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 8. EMM Functional Requirements

Req. UID	Requirement Text
EMM-1	The EMM capability shall enforce the use of an agency defined catalog of mobile applications for distribution to mobile devices.
EMM-2	The EMM capability shall block access to application stores, based on agency policy.
	Guidance: Application stores include commercial application catalogs (i.e., Google Play, Apple App Store.).
EMM-3	The EMM capability shall block access to pre-installed mobile applications, based on agency policy.
	Guidance: "pre-installed" mobile applications are those applications on the mobile device that are installed when the device is acquired "out of the box".
EMM-4-1	The EMM capability shall enforce an agency-defined Deny List of mobile applications, using any combination of the following mobile application characteristics: • Mobile application manufacturer • Mobile application version • Mobile application hash
	Guidance: "Enforce" is a tool specific action, as defined by the agency, which may include the following: prevention of installation of the mobile application, disabling the mobile device, and/or recording the non-compliance state in the EMM console.
EMM-4-2	The EMM capability shall record the mobile device as "out of compliance" upon detection of a mobile application on the Deny List.
	Guidance: "Out of compliance" is a generic term for a device state that is in violation of agency and/or Federal policy, as evaluated by the CDM capability.
EMM-4-3	The EMM capability shall enforce an agency-defined Allow List of mobile applications, using any combination of the following mobile application characteristics: • Mobile application manufacturer • Mobile application version • Mobile application hash
EMM-4-4	The EMM capability shall record a mobile device as "out of compliance", upon detection of a mobile application not on the Allow List.
	Guidance: "Out of compliance" is a generic term for a device state that is in violation of agency and/or Federal policy, as evaluated by the CDM capability.
EMM-5	The EMM capability shall block access to agency-defined resources from mobile devices that are out of compliance, based on agency policy.
	Guidance: "agency resources" generically include agency defined enterprise assets such as email, file stores, enclaves/networks, agency web applications, etc. The intent of this functionality is to incorporate a "network access control" (NAC)-like function into the EMM capability.
EMM-6-1	When configured by the administrator, the EMM capability shall deploy mobile applications to specific enrolled mobile devices without end user intervention.
	Guidance: After a mobile device is enrolled, it is managed with active policy settings from the administrator.
EMM-6-2	When configured by the administrator, the EMM capability shall update mobile applications on specific enrolled mobile devices without end user intervention.
EMM-6-3	When configured by the administrator, the EMM capability shall remove mobile applications from specific enrolled mobile devices without end user intervention.
EMM-6-4	When configured by the administrator, the EMM capability shall deploy mobile applications to a group of enrolled mobile devices without end user intervention.

Req. UID	Requirement Text
EMM-6-5	When configured by the administrator, the EMM capability shall update mobile applications on a group of enrolled mobile devices without end user intervention.
EMM-6-6	When configured by the administrator, the EMM capability shall remove mobile applications from a group of enrolled mobile devices without end user intervention.
EMM-6-7	When configured by the administrator, the EMM capability shall remove agency-installed mobile applications and associated data when mobile devices are unenrolled.
EMM-7-1	The EMM capability shall log attempted and actual violations of EMM configurations implemented on mobile devices.
EMM-7-2	The EMM capability shall log all administrative actions taken on the EMM console.
EMM-7-3	Based on agency policy, the EMM capability shall display real-time alerts on the mobile device for violations of EMM configurations implemented on the mobile device.
	Guidance: "real-time alerts" is a generic term that represents a tool/technology "best effort" to get the alert (i.e., notification) unambiguously visible to the end-user/administrator as soon as possible, which is acceptable to the capability owner (e.g., Agency).
EMM-7-4	The EMM capability shall generate real-time alerts on the EMM console for violations of EMM configurations implemented on mobile devices.
	Guidance: "real-time alerts" is a generic term that represents a tool/technology "best effort" to get the alert (i.e., notification) unambiguously visible to the end-user/administrator as soon as possible, which is acceptable to the capability owner (e.g., Agency).
EMM-8-1	The EMM capability shall maintain a timely, updated inventory of mobile applications installed on each mobile device.
EMM-8-2	The EMM capability shall report an inventory of mobile applications installed on each mobile device.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported inventories are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).
EMM-8-3	The EMM capability shall maintain a timely, updated mobile device inventory that includes a unique device ID, mobile device model, manufacturer, OS, OS version, and the compliance state of each mobile device.
	Guidance: Mobile device model should be inclusive of the mobile device type (i.e., phone or tablet) if not specified by the model name/number directly.
EMM-8-4	The EMM capability shall report a mobile device inventory that includes a unique device ID, mobile device model, manufacturer, OS, OS version, and the compliance state of each mobile device.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported inventories are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards). Compliance state is intended to reflect whether a mobile device possesses any known defects as defined by agency and/or Federal policy (e.g., "out of compliance")
EMM-9	The EMM capability shall permit/deny end user access to mobile applications and data on the mobile device based on the network connected to the mobile device, according to agency policy.
EMM-10-1	Based on agency policy, the EMM capability shall configure settings on mobile devices to control permissions to the mobile device's services, resources, and data on a per mobile application basis.
	Guidance: Mobile device services examples include location services, mobile devices resources include device functionality such as microphone, biometric sensors, etc.
EMM-10-2	The EMM capability shall enforce configuration settings related to mobile application policies on a per end user basis.
	Guidance: Requirement 10-1 outlines the potential configuration settings to be incorporated into agency defined mobile application centric policies.

Req. UID	Requirement Text
EMM-10-3	The EMM capability shall enforce mobile application policies on a per end user group basis.
	Guidance: Requirement 10-1 outlines the potential configuration settings to be incorporated into agency-defined mobile application centric policies.
EMM-11-1	The EMM capability shall integrate with the Mobile Application Vetting (MAV) capability to incorporate mobile application security information to allow EMM to implement mitigations for mobile applications with unacceptable reputation scores.
	Guidance: The MAV capability provides mobile application reputation scores. Agency policy determines the range of acceptable scores and the mitigation actions for mobile applications with unacceptable reputations scores. This requirement applies to ensuring interoperability with an existing or future MAV solution only; establishment of a new MAV solution, governance, or integration to a MAV solution by the SI is out of scope.
EMM-11-2	The EMM capability shall integrate with the Mobile Threat Defense (MTD) capability to allow for enhanced mitigation against mobile threats.
	Guidance: The MTD capability provides malicious activity alerts based upon active threats and vulnerabilities on the mobile device. Agency policy determines the mitigation actions against the malicious activities. This requirement applies to ensuring interoperability with an existing or future MTD solution only; establishment of a new MTD solution, governance, or integration to a MTD solution by the SI is out of scope
EMM-12	The EMM capability shall permit/deny end user access to mobile applications and data on the mobile device based on the physical location of the mobile device, according to Agency policy.
EMM-13	The EMM capability shall permit/deny end user access to mobile applications and data on the mobile device based on time of day, according to Agency policy.
EMM-14-1	The EMM capability shall perform a full wipe of mobile device data upon administrator command.
	Guidance: A full wipe of mobile devices includes deletion of all stored data within a system's user partition (e.g., all storage areas that are user accessible or utilized to support user functionality).
EMM-14-2	The EMM capability shall perform a partial wipe of mobile device data upon administrator command.
	Guidance: A partial wipe of mobile devices includes removal of all security containers, profiles, mobile applications, data, and certificates that were provisioned to the mobile device by the EMM capability.
EMM-14-3	The EMM capability shall wipe the mobile device automatically if any of the following criteria are met and defined within agency policy: • Agency-defined maximum number of failed login attempts is reached • Subscriber identity module (SIM) card is changed or removed • Agency-defined maximum period without communication with the EMM is reached
EMM-14-4	The EMM capability shall delete selected mobile applications and associated data on mobile devices upon administrator command.
EMM-14-5	The EMM capability shall perform a “factory reset” operation to include cryptographically erasing all end user data upon administrator command.
	Guidance: A “factory reset” operation is intended to put the mobile device into its original “factory” (i.e., out of the box) condition. Cryptographic Erase definition: https://csrc.nist.gov/glossary/term/cryptographic-erase
EMM-15	The EMM capability shall lock mobile devices upon administrator command, requiring administrator unlock.
EMM-16	The EMM capability shall continuously monitor mobile devices’ state of compliance and, based upon agency policy, permit/deny the mobile device’s access to agency-defined mobile applications and associated data.
EMM-17	The EMM capability shall lock mobile devices upon administrator command, requiring the end user to unlock the mobile device.

Req. UID	Requirement Text
EMM-18	The EMM capability shall lock mobile devices automatically requiring end user or administrator unlock, depending on agency policy, if any of the following occur: • Agency-defined maximum number of failed login attempts is reached • SIM card is changed or removed • Agency-defined maximum period without communication with the EMM is reached
EMM-19	The EMM capability shall ensure that a mobile device passes compliance checks based on the below characteristics, as defined within agency policy, prior to accessing agency resources: • OS version • OS patch level • Jailbreak status • Device configuration settings • Device encryption status
EMM-20	The EMM capability shall enforce full mobile device encryption.
EMM-21	The EMM capability shall record a mobile device as "out of compliance" if full device encryption is not enabled.
	Guidance: "Out of compliance" is a generic term for a device state that is in violation of agency and/or Federal policy, as evaluated by the CDM capability.
EMM-22-1	When configured by an administrator, the EMM capability shall import cryptographic keys into the secure key storage on the mobile device.
EMM-22-2	The EMM capability shall destroy imported cryptographic keys in the secure key storage on the mobile device, based on Agency policy.
EMM-22-3	When configured by the administrator, the EMM capability shall import cryptographic certificates into the Trust Anchor Database on the mobile device.
EMM-22-4	The EMM capability shall remove cryptographic certificates in the Trust Anchor Database on the mobile device, based on Agency policy.
EMM-23-1	The EMM capability shall configure virtual private network (VPN) connections on mobile devices, based on Agency policy.
EMM-23-2	The EMM capability shall enforce cryptographic settings and algorithms for encrypting mobile device secure communications, based on Agency policy.
EMM-24	The EMM capability shall enforce end user and mobile application access to mobile device sensors and radios, based on Agency policy.
	Guidance: Mobile device sensors include camera, microphone, GPS, and biometric sensors.
EMM-25	The EMM capability shall enforce cryptographic settings and algorithms for encrypting mobile device data at rest, based on Agency policy.
EMM-26	The EMM capability shall implement agency-defined policies based on the mobile device characteristics of mobile device type, manufacturer, model, OS, and location for the purposes of enforcing the following configurations when defined within agency policy: • Enable or disable network interfaces • Block or permit access to hardware • Block or permit access to device services • Application of encryption settings for data at rest and in transit
EMM-27	The EMM capability shall prevent mobile device access to public cloud resources, based on Agency policy.
	Guidance: Examples of cloud resources include Dropbox, Office 365, and Gmail. Public means that the resource is not managed by the Agency.
EMM-28	The EMM capability shall remove the following data associated with the agency when the mobile device is unenrolled: • Agency defined EMM policies • End user profiles • Agency managed mobile applications and associated data • End user data

Req. UID	Requirement Text
EMM-29	The EMM capability solutions shall ensure mobile device boot attestations are successfully executed prior to allowing mobile device access to agency resources.
EMM-30	The EMM capability shall enforce an agency-defined Allow list of mobile devices by: • Vendor and model • An agency-defined UID
	Guidance: Mobile device model should be inclusive of the mobile device type (i.e., phone or tablet) if not specified by the model name/number directly. "Enforce" is a tool specific action, as defined by the agency, which may include the following: disabling the mobile device, preventing access to agency resources, and/or recording the non-compliance state in the EMM console. A UID can be any agency-defined combination of mobile attributes (certificate, serial number, etc.) that can be implemented in the EMM capability.
EMM-31	The EMM capability shall enforce mutual, secure authentication mechanisms to and from the mobile device for device management communications.
	Guidance: Device Management communications include EMM policy/configuration related updates, issued commands (e.g., push software, remove mobile applications), inventory/status/compliance reporting, etc.
EMM-32-1	The EMM capability shall digitally sign mobile device policies and updates when they are issued to mobile devices.
EMM-32-2	The EMM capability shall require signature verification before policy and updates are applied to mobile devices.
EMM-33	The EMM capability shall configure wireless local area network (WLAN) profiles on mobile devices, based on Agency policy.
EMM-34	The EMM capability shall configure Bluetooth profiles on mobile devices, based on Agency policy.
EMM-35	The EMM capability shall enforce end user authentication when the mobile device is in the locked state.
EMM-36	The EMM capability shall transition the mobile device to the locked state when the Agency-defined inactivity time-out period is reached.
EMM-37	The EMM capability shall enable/disable display notification of the following when the mobile device is in the locked state, based on agency policy: • Email notifications • Calendar appointments • Contact associated with phone call notification • Text message notification • Other mobile application-based notifications
EMM-38	The EMM capability shall enforce an authentication method for end user access to mobile devices, using the one of the following methods as defined within agency policy: • Password/PIN • Biometric • Certificate-based • Multi-factor
EMM-39	The EMM capability shall enforce the following agency-defined password characteristics when the password authentication method is implemented: • Minimum password length • Minimum password complexity • Maximum password lifetime
	Guidance: Additional password characteristics could include enforcing password history, which involves ensuring no reuse of the last 'n' passwords, e.g., n=10.

Req. UID	Requirement Text
EMM-40	The EMM capability shall enforce an authentication method for performing administrative functions, using the one of the following methods as defined within agency policy: • Password/PIN • Biometric • Certificate-based • Multi-factor
EMM-41-1	The EMM capability shall create end user profiles for mobile devices, using agency-defined user data.
EMM-41-2	The EMM capability shall create end user groups for mobile devices, based on agency policy.
EMM-41-3	The EMM capability shall implement a directory of authorized users using an agency-defined combination of end user profiles and/or end user groups.
EMM-41-4	The EMM capability shall automatically prevent end users from accessing the mobile device when the end users are deactivated from the directory of authorized users.
EMM-42	The EMM capability shall permit/deny end user access to mobile applications and data on the mobile device based on agency defined usage patterns.
	Guidance: Usage pattern includes user, device, app and system information for use in creating analytics (i.e., user behavior analytics) that describe overall expected/unexpected usage within the managed mobile environment.
EMM-43	The EMM capability shall enforce end user and mobile application access to external storage on mobile devices, based on Agency policy.

2.2.5.1.1 Mobile Threat Defense Sub-Capability[23]

The Mobile Threat Defense (MTD) sub-capability enables an agency to detect and address malicious mobile applications, network-based attacks, improper configurations and known vulnerabilities in mobile apps or the mobile devices to protect the agency. The MTD sub-capability is scoped to provide functionality applicable to mobile devices that are in scope for CDM[24] and have an EMM capability implemented.

As described in the NIST 800-124 Revision 2, MTD systems often run an agent on the device—typically a mobile application (app)—and may also initiate analysis and learning on external platforms. MTD systems provide real-time monitoring, assessing apps after deployment to a mobile device as well as during runtime. MTD systems can detect and protect the mobile device, apps, and end-user against attacks via the wireless network. MTD systems typically work in conjunction with a backend server to detect and defend against security threats.

The MTD sub-capability integrates with the EMM capability to enable alerts from MTD to trigger automatic or manual remediation of detected vulnerabilities or automatically/manually quarantine apps or devices. The MTD sub-capability protects at the device, network, and app levels to counter malicious attacks.

The following are the CDM MTD functions:

1. **Detect and Mitigate Malware** function detects and mitigates the detected malware. Malware (also known as malicious apps or malicious code), as defined by NIST SP 800-53, represent software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system – malicious apps may steal user data, commit financial fraud, negatively impact device performance, or cause other damage. Examples include a virus, worm, Trojan horse, spyware or other code-based entity that infects a host. Some mobile apps may not necessarily be malicious but pose a risk to the enterprise. For example, side-loaded apps pose a risk since they have not been vetted through

[23] NIST SP 800-124 Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. National Information Assurance Partnership, *Protection Profile for Mobile Device Fundamentals 1*.
[24] Within CDM mobile devices are government furnished, portable devices that run a mobile based operating system (e.g., Android, iOS, etc.). See the program's integrated data dictionary (AV-2) for more information.

an App Store. An app that collects location data may pose risks by exposing potentially sensitive data.

2. **Detect Anomalous Behavior** function monitors mobile app and user behavior to detect anomalies (e.g., exfiltration of large amounts of data to unknown server or suspicious interactions with other apps) based on non-signature-based algorithms.
3. **Detect and Mitigate Mobile Device Vulnerability** function identifies the vulnerabilities for the device, based on model, OS version, carrier version, and security patch level.
4. **Detect and Mitigate Mobile Network Attack** function identifies, prevents, or remediates network attacks and malicious network behaviors.
5. **Detect Sideloaded Apps** function detects the installing of an app on a mobile device without downloading it from an authorized app store. For example, the user may install an app that has been manually downloaded, which can introduce malware on the device.
6. **Enforce Mobile Safe Browsing** function detects and helps to prevent downloading of additional code at runtime, phishing attacks, and connecting to malicious domains.
7. **Log and Alert on MTD events** function records the actions taken by the MTD capability and provides alerts.
8. **Remediate Mobile Risks through Integration with EMM** function restricts access to enterprise resources through integration with EMM based on a mobile device's risk posture.
9. **Maintain and Report CDM Data** function makes updated MTD data available and provides it to the Agency Dashboard

The following is a non-exclusive list of tool functionalities that support the MTD functional requirements:

Tool Category Name	Summary of Functionality
Mobile threat defense (or mobile threat management) tools	Detection of the presence of malicious apps or software, malicious activity, and connections to denied websites or networks.
Enterprise Mobility Management tools	Enables administrators to enforce required security measures, remotely configure applications, and securely grant access to data

The following is a non-exclusive list of tools that MTD may integrate with:

Tool Category Names	Summary of Functionality
Enterprise Mobility Management (EMM) tools (include Mobile Device Management tools and Mobile Application Management tools)	Enables administrators to enforce required security measures, remotely configure applications, and securely grant access to data.
Unified Endpoint Management (UEM) tools	Manages all the endpoint devices within an organization from a central location, such as: security updates, patch management, HW and SW inventory tracking, logging, mobile device management, software and OS deployment, and workstation remote control.
Security Information and Event Management (SIEM) tools	Logs CSM administrator actions and CSM management.

2.2.5.1.2 MTD Functional Requirements

This section provides functional requirements for the MTD capability. The "shall" statements included in this set of requirements in Table 9 often require agency policy inputs to accurately develop machine readable policies (i.e., configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 9. MTD Functional Requirements

Summary	Description
Detect and Mitigate Malware	
MTD-1-3	The MTD capability shall block the download of malware onto mobile devices.

Summary	Description
	Guidance: Malware (i.e., Malicious apps) are apps that intend to negatively impact the device or data on the device. Detection of malware on a mobile device constitutes a defect. Malware is generally detected using signature definitions or behavioral analysis. An example behavioral analysis technique employs lists of behaviors known to be (1) malicious (e.g., leaking data, requesting excessive permissions) and (2) expected and acceptable use patterns, then comparing the activity on the mobile devices against these behaviors for anomalies. These lists can be specific to the MTD vendor and are expected to be updated as needed, using an authoritative source provided by the MTD vendor or integrated threat intelligence feeds provided as part of the capability.
MTD-1-2	The MTD capability shall block the execution of known malware onto mobile devices.
	Guidance: Malware (i.e., Malicious apps) are apps that intend to negatively impact the device or data on the device. Detection of malware on a mobile device constitutes a defect. Malware is generally detected using signature definitions or behavioral analysis. An example behavioral analysis technique employs lists of behaviors known to be (1) malicious (e.g., leaking data, requesting excessive permissions) and (2) expected and acceptable use patterns, then comparing the activity on the mobile devices against these behaviors for anomalies. These lists can be specific to the MTD vendor and are expected to be updated as needed, using an authoritative source provided by the MTD vendor or integrated threat intelligence feeds provided as part of the capability.
MTD-1-1	The MTD capability shall detect an instance of malware when an app, known to be malware, is installed on a mobile device.
	Guidance: Malware (i.e., Malicious apps) are apps that intend to negatively impact the device or data on the device. Detection of malware on a mobile device constitutes a defect. Malware is generally detected using signature definitions or behavioral analysis. An example behavioral analysis technique employs lists of behaviors known to be (1) malicious (e.g., leaking data, requesting excessive permissions) and (2) expected and acceptable use patterns, then comparing the activity on the mobile devices against these behaviors for anomalies. These lists can be specific to the MTD vendor and are expected to be updated as needed, using an authoritative source provided by the MTD vendor or integrated threat intelligence feeds provided as part of the capability.
Detect Anomalous Behavior	
MTD-2-1	The MTD capability shall analyze app behavior to detect anomalous behavior as triggered by potential sensitive data exfiltration, based on agency policy.
	Guidance: "Analyze" is intended to be fulfilled by technology-specific solutions but is generally met by real-time continuous monitoring of app and user activity to detect malicious apps/activities (e.g., lack of encryption, interactions between apps, data use) based on non-signature-based techniques. Machine learning algorithms may be useful to implement this requirement. Agency policy should identify the types of sensitive data, how it can be transmitted, and to which destinations.
MTD-2-2	The MTD capability shall prevent unauthorized sensitive data exfiltration by apps, based on agency policy.
	Guidance: This requirement is intended to prevent agency data loss upon detection of anomalous behavior described in MTD-2-1. Agency policy should identify the types of sensitive data, how it can be transmitted, and to which destinations.
MTD-2-3	The MTD capability shall detect anomalous app behavior when the app attempts to access any of the following to end user privacy information: • Mobile device location information • Mobile device details (installed apps/OS, device make/model) • Personally Identifying Information (end user name, email, phone number)
	Guidance: Examples of anomalous app behavior include collecting/revealing device location and user or device details, including when unauthorized to do so. The intent is for the MTD capability to be able to automatically detect these events with minimal administrator/policy input. Machine learning algorithms may be useful to implement this requirement.
MTD-2-4	The MTD capability shall detect anomalous app behavior as triggered by prohibited file system access, based on agency policy.

Summary	Description
	Guidance: The intent is for agency policy to dictate the MTD configuration regarding what constitutes prohibited file system access. In the absence of a codified agency policy, technology vendor defaults may be employed as de facto agency policy.
MTD-2-5	The MTD capability shall detect anomalous app behavior as triggered by communications with known command and control servers.
	Guidance: Monitoring apps utilizing machine learning algorithms may be useful to implement this requirement.
MTD-2-6	The MTD capability shall detect connections to unsecure networks, based on agency policy.
	Guidance: This could be implemented using an allow list of "secure" networks and handling all other networks as "unsecure". By default, a Wi-Fi network should be considered unsecure when the network does not require a secure protocol such as WPA or WPA2 password (e.g., an Open/Public Network). Out of the box (OOTB) functionality generally supports the allow/deny lists.
MTD-2-7	The MTD capability shall detect connections to unsecure cloud services, based on agency policy.
	Guidance: This could be implemented using an allow list of "secure" cloud services and handling all other cloud services as "unsecure". OOTB functionality generally supports the allow/deny lists.
Detect and Mitigate Mobile Device Vulnerability	
MTD-3-1	The MTD capability shall detect a mobile device that has been modified to provide root level access to the underlying OS.
	Guidance: Detection of a rooted or jailbroken device constitutes a defect.
MTD-3-2	The MTD capability shall detect a mobile device that has a malicious profile installed.
	Guidance: A profile is set of configuration settings on a mobile device. It can include email, calendar, and passcode restriction settings. If a malicious profile gets installed, it can result in misconfigurations that could lead to device or data compromise. Detection of a malicious profile constitutes a defect. *An example of a malicious profile is one that allows attackers to bypass access restrictions by installing incorrect security-related configuration settings that allow the compromise of the device and sensitive information. Attackers may install the malicious profile by creating a link to the malicious profile and executing a phishing attack to start the installation.*
MTD-3-3	The MTD capability shall report on the mobile OSs, version, and security patch level and associated mobile vulnerabilities.
	Guidance: The MTD capability leverages information provided by vendor as well as collaborative information provided by industry threat feeds to show the mobile OSs and the vulnerabilities (i.e., CVEs) for each version and security patch level. Mobile vulnerabilities constitute a defect.
MTD-3-4	The MTD capability shall block apps that perform actions that are determined to be high risk for data leakage, based on agency policy.
	Guidance: This requirement may be met by performing static, dynamic, and behavioral analysis. MTD-3-4 addresses the requirement to detect apps that can perform actions that are determined to be high risk for data leakage.
MTD-3-5	Based on agency policy, the MTD capability shall automatically detect apps that request permissions that are determined, by the MTD vendor, to be high risk for data leakage.
	Guidance: Data leakage may consist of location, contact, or other sensitive information that is leaving the device unintentionally, unknowingly, or without authorization. This requirement may be met by performing static, dynamic and behavioral analysis. This requirement is intended to be uniquely met by MTD technology vendors OOTB with minimal input needed from agencies (or policies).
MTD-3-6	Based on agency policy, the MTD capability shall automatically block apps that request permissions that are determined, by the MTD vendor, to be high risk for data leakage.

Summary	Description
	Guidance: This requirement may be met by performing static, dynamic and behavioral analysis. Agency policy is intended to dictate if apps are automatically blocked or not. This requirement is intended to be uniquely met by MTD technology vendors OOTB with minimal input needed from agencies (or policies).
MTD-3-7	The MTD capability shall automatically detect apps that can perform actions that are determined, by the MTD vendor, to be high risk for data leakage.
	Guidance: Data leakage may consist of location, contact, or other sensitive information that is leaving the device unintentionally, unknowingly, or without authorization. One way to meet this requirement is to perform analysis of the app code. This requirement is intended to be uniquely met by MTD technology vendors OOTB with minimal input needed from agencies (or policies).
MTD-3-8	The MTD capability shall detect and alert on mobile device misconfigurations.
	Guidance: An example of a misconfiguration is a device with person-in-the-middle attack prevention disabled or a device with side-loaded app detection disabled. EMM establishes the configurations while MTD detects/alerts of misconfigurations. Detected misconfigurations constitute a defect.
MTD-3-9	The MTD capability shall detect OS or kernel level attacks.
	Guidance: The intent is for the MTD technology to monitor for these types of attacks generically, which can demonstrated by decomposition and demonstration of the technology's ability to detect one example of this archetype. For other examples please refer to the MITRE Mobile Attack Framework[25] (e.g., Technique ID T1398).
MTD-3-10	The MTD capability shall prevent installation of malicious profiles.
	Guidance: A profile is a set of configuration settings on a mobile device. It can include email, calendar, and passcode restriction settings. If a malicious profile gets installed, it can result in misconfigurations that could lead to device or data compromise. *An example of a malicious profile is one that allows attackers to bypass access restrictions by installing incorrect security-related configuration settings that allow the compromise of the device and sensitive information. Attackers may install the malicious profile by creating a link to the malicious profile and executing a phishing attack to start the installation. (Reference NIST SP 800-124 Rev. 2)*
Detect and Mitigate Mobile Network Attack	
MTD-4-1	The MTD capability shall prevent person-in-the-middle attacks.
	Guidance: Examples of person-in-the-middle attacks are SSL interception (a malicious proxy that routes traffic through an attacker network) and SSL stripping (an attack that obtains a connection and rewrites content in plaintext to expose encrypted traffic).
MTD-4-2	The MTD capability shall prevent cellular network attacks.
	Guidance: Detects threats deriving from cellular network vulnerabilities such as the ones in the SS7 protocol or the false base station (aka Stingray) attack.
MTD-4-3	When threats or unsecure connections are detected, the MTD capability shall mitigate mobile network attacks by securing the mobile traffic.
	Guidance: Example methods for securing the traffic include the use of VPN or blocking the traffic. This can be accomplished by MTDs that have VPNs built in that can be dynamically triggered.
Detect Sideload Apps	
MTD-5-1	The MTD capability shall detect sideloaded apps.
	Guidance: "Sideloaded apps" are apps that are installed without using an authorized mobile application store, which is based upon agency policy. Detection of sideloaded apps can be accomplished using an allow list of authorized app stores.

[25] Matrix - Mobile | MITRE ATT&CK® MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Summary	Description
MTD-5-2	The MTD capability shall enforce an allow list of sideloaded apps which is based on agency policy.
Enforce Mobile Safe Browsing	
MTD-6-1	The MTD capability shall detect when the mobile device downloads additional code at app runtime.
	Guidance: Examples of additional code include libraries that are downloaded at runtime as opposed to those that are provided with the app.
MTD-6-2	The MTD capability shall detect, using non-signature-based techniques, when the app navigates to phishing sites.
	Guidance: This is generally accomplished by analyzing the characteristics of the URL to identify phishing sites. An example of this type of URL is the one disguised using a shortening service so that the user cannot see the full URL that helps to identify potential phishing sites. Machine learning algorithms may be useful to implement this requirement.
MTD-6-3	The MTD capability shall prevent phishing attacks received that includes all of the following methods: • Mobile apps utilized for e-mail or messaging, • Web browsing, • SMS/MMS text messaging
	Guidance: This is generally accomplished using a list of known malicious URLs. This may also be accomplished by analyzing the characteristics of the URL as mentioned in the guidance for MTD-6-2.
MTD-6-4	The MTD capability shall detect malicious URLs using deny lists based upon agency policy.
	Guidance: Sources of deny list information are intended to come from multiple sources including agency policy and MTD technology OOTB functionality.
MTD-6-5	The MTD capability shall detect malicious URLs using non-signature-based techniques.
	Guidance: Malicious URLs may be identified using the characteristics of the URL. Machine learning algorithms may be useful to implement this requirement.
MTD-6-6	The MTD capability shall block access to malicious domains based on deny lists.
	Guidance: Malicious domains can be reached by any network protocol (e.g., SMTP, IMAP, FTP, HTTP/HTTPS). Sources of deny list information are intended to come from multiple sources including agency policy and MTD technology OOTB functionality. The intent is for MTD-6-4, MTD-6-5 to protect against web-browsing activity while MTD-6-6 has a broader protection scope to other communications and protocols.
MTD-6-7	When configured by the administrator, the MTD capability shall automatically protect Over-The-Air connections made by the mobile device, based on agency policy.
	Guidance: An example of protection in this case is automatically encrypting traffic when connecting to an open Wi-Fi network. Agency policy shall dictate the applicability of automatically protecting over-the-air connections.
Log and Alert on MTD Events	
MTD-7-1	The MTD capability shall log detected anomalous behavior of the mobile device user, based on agency policy.
	Guidance: The intent of this requirement is to implement a logging function by virtue of a MTD agent and MTD console of any anomalous mobile device user activity. Anomalous behavior is intended detected by OOTB functionality and tailored based on agency needs. "Anomalous" behavior subject to logging is based on an agency policy-based tailored configuration which can be decomposed to include functions/events in the MTD capability requirement MTD-9-2.
MTD-7-2	The MTD capability shall log detected anomalous behavior of the mobile device, based on agency policy.

Summary	Description
	Guidance: The intent of this requirement is to implement a logging function by virtue of a MTD agent and MTD console of any anomalous mobile device activity. Anomalous behavior is intended detected by OOTB functionality and tailored based on agency needs. "Anomalous" behavior subject to logging is based on an agency policy-based tailored configuration which can be decomposed to include functions/events in the MTD capability requirement MTD-9-2.
MTD-7-3	The MTD capability shall generate real-time alerts, based on agency policy.
	Guidance: Real-time alerts can be sent to the user for threats such malicious URLs sent via email or text, "real-time alerts" is a generic term that represents a tool/technology "best effort" to get the alert (i.e., notification) unambiguously visible to the end-user/administrator as soon as possible. Agency policies should determine when/if real-time alerts are triggered (e.g., detection of malware, rooted devices, anomalous activity, etc.).
Remediate Mobile Risks through integration with EMM	
MTD-8-1	The MTD capability shall integrate with the EMM capability to restrict access to agency-defined resources, based on the agency's policy for the mobile device's risk posture.
	Guidance: MTD provides risk posture to EMM by transmitting vulnerability and risk (potential compromise) information to the EMM. Risk posture may be determined by the OS version, OS patch level, jailbreak status, configuration policy, or device encryption status, but is ultimately determined by the Agency's policy on what conditions constitute too much risk for allowing access to any specified agency resource.
MTD-8-2	When sideloaded apps are detected, the MTD capability shall integrate with the EMM capability to have the EMM capability mitigate this defect.
	Guidance: "Sideloaded apps" are apps installed without using an authorized app store. MTD identifies the sideloaded apps to the EMM which in turn provides a mitigation. Examples of mitigation actions include uninstalling the app, adding the app to the app deny list, and removing the app from the app allow list.
MTD-8-3	When malware is detected, the MTD capability shall integrate with the EMM capability to have the EMM capability mitigate this defect.
	Guidance: MTD identifies the malware (for example, illegitimate side-loaded apps from untrusted sources, legitimate apps being employed to conduct malicious activities, or any app that intends to negatively impact the device or data on the device) and provides alerts to the EMM which in turn provides a mitigation. Examples of mitigation actions include uninstalling the app, adding the app to the app deny list, removing the app from the app allow list, proactively shutting down attacks on-device without network connectivity required, and isolating compromised devices from the network.
MTD-8-4	When integrated with the EMM, the MTD capability shall have the EMM capability add apps to the deny list automatically or upon administrator input, based on agency policy, the apps that can perform actions that are detected to be high risk for data leakage.
	Guidance: One way to meet this requirement is to use analysis of the app code. The deny-list updates are implemented through integration with EMM. Agency policy dictates if the deny-list addition is manual or automated. The MTD capability is intended to determine/recommend app "actions" that are high risk for data leakage, OOTB. See MTD-3-4 for more details.
MTD-8-5	When integrated with the EMM, the MTD capability shall have the EMM capability add apps to the deny-list automatically or upon administrator input, when the app requests permissions that are determined to be high risk for data leakage based upon agency policy.
	Guidance: This requirement may be met by performing static, dynamic and behavioral analysis. The deny list updates are implemented through integration with EMM. Agency policy dictates if the deny list addition is manual or automated along with what is "high risk", if different from an OOTB configuration. See MTD-3-5 for more details.
Maintain and Report CDM Data	
MTD-9-1	The MTD capability shall maintain a repository of detected defects and anomalies for mobile devices on the Agency network.
	Guidance: Refer to previous MTD requirements regarding the scope of detected defects and anomalies.

Summary	Description
MTD-9-2	The MTD capability shall report the detected defects on mobile devices on the Agency network that includes all of the following: • Devices detected to be jailbroken/rooted • Detected instances of malware • Detected instances of sideloaded apps • Detected mobile device misconfigurations • Detected mobile vulnerabilities as CVEs
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported inventories are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).

2.3 Identity and Access Management (IdAM) Capability Area

The IdAM capability area addresses "Who is on the Network" to strengthen management of users and accounts on Agency networks. The IdAM capabilities focus on identifying Agency users, and ensuring that they have been properly vetted, trained, and authenticated.

The four IdAM component capabilities are:

- **TRUST Requirements** – The CDM TRUST capability reduces the probability of loss in availability, integrity, and confidentiality of data by ensuring that only properly vetted users are given access to credentials and systems commensurate with their role. This includes elevated privileges and special security roles. The vetted trust level is properly monitored and renewed, per agency policies and applicable statutes.
- **BEHAVE Requirements** – The CDM BEHAVE capability ensures that an authorized user exhibits the appropriate behavior for their role. For CDM, appropriate security-related behavior is defined as actions that have been assigned, explained, and "agreed to" by the user via user agreements, training, job requirements, or similar methods. This capability provides an Agency with insight into risks associated with non-conformance with policies for accessing systems and data by authorized users.
- **CRED Requirements** – The CDM CRED (credentials and authenticators) capability ensures that account credentials are assigned to, and are used only by, authorized users or services to access agency systems, services, and facilities. CRED binds a type of credential or authenticator to an identity established in TRUST with a level of assurance and is used to grant logical access.
- **PRIV Requirements** – The purpose of the PRIV capability is to ensure that privileges for logical access are assigned to authorized people or accounts that require authorized access for job functions. This capability is dependent on the existence of a set of attributes that denote roles or characteristics that require or restrict specific privileges per policy. This capability provides the agency with insight into risks associated with authorized users being granted excessive privileges to facilities, systems, and information at any level of sensitivity. PRIV also has two sub-capabilities, ILM and PAM. ILM enables automation throughout the IdAM lifecycle by adjusting information in connected repositories to address changing positions and responsibilities.

The Data Dictionary within the CDM Data Model Document (DMD) defines the specific attributes for IdAM. The IdAM capabilities extract the actual state attributes from Agency authoritative sources, which maintain accurate, current attributes. The possible authoritative sources include existing Human Resources (HR) (i.e., Personnel), Learning Management, clearance or investigation management, and IdAM systems. For some Agencies that are geographically dispersed or have major components, these sources may span multiple systems and not be consolidated.

A Policy Administrative Point (PAP) is the interface to manage the machine-readable policies (desired state). The Policy Decision Point (PDP) is the mechanism that compares the actual state with the desired state and detects defects that require attention. The PRIV PAM sub-capability provides a PEP for making privileged user authentication and access decisions.

2.3.1 TRUST Capability

The CDM TRUST capability reduces the probability of loss in availability, integrity, and confidentiality of data by ensuring that only properly vetted users are given access to credentials and systems commensurate with their role. This includes elevated privileges and special security roles. The vetted trust level is properly monitored and renewed, per agency policies and applicable statutes. The TRUST capability will apply only to in-scope users (employees and contractors, who will each have a PIV card).
The following are the functions of the TRUST capability:

- **Establish Agency TRUST desired state in machine-readable policies** stores the Agency-defined desired-state TRUST policies in machine-readable form. TRUST maintains the desired state.
- **Collect TRUST information from authoritative sources** collects actual state information from the TRUST capability authoritative sources which are existing systems that vary by Agency. These contain attributes regarding TRUST background investigations, expiration date, etc.
- **Compare Agency actual state to TRUST policy** compares Agency desired state with collected actual state and identifies defects. This is the PDP.
- **Display TRUST information and generate reports locally** provides the administrator the ability to display TRUST information and generate reports.
- **Report TRUST information to Agency dashboard** reports TRUST information and TRUST defects to the Agency Dashboard.

The TRUST capability must integrate with external systems that are authoritative sources of actual state information such as:

- Facilities access systems to identify location of the user
- Clearance systems or equivalent

The authoritative sources for the TRUST capability vary by Agency but contain primary attributes regarding background investigations and any related determinations to ensure they are "current" (as specified in the Federated Identity, Credential, and Access Management [FICAM] roadmap [26]) and according to the "currency" criteria of the Agency. The basis of such determinations is:

- Security clearance determination
- Suitability determination
- Fitness determination
- Non-disclosure agreements
- Financial disclosure agreements

The TRUST capability will help ensure that every user meets the required trust attributes, is periodically rescreened to revalidate trustworthiness, and does not have attributes that violate the Agency's policies.

[26] IDManagement.gov,"Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance," December 2011

The following is a non-exclusive list of tool functionalities that support TRUST capability:

Tool Category Name	Summary of Functionality
Audit reporting tools	Enables evaluation of the company's compliance with regulations, as well as measuring their performance against an established set of criteria. These are done to identify security problems and gaps, establish a security baseline, compliance with internal and external policies and requirements, and determine if security training is adequate
Policy management tools	Manages the creation review, and implementation of corporate policies across the company, ensuring compliance with corporate standards such as security, privacy, behavior, or trust

2.3.1.1 TRUST Functional Requirements

This section provides functional requirements for the TRUST capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 10. TRUST Functional Requirements

Req. UID	Requirement Text
Establish Agency TRUST desired state in machine-readable policies	
TRUST-1-1	The TRUST capability shall implement TRUST policies in machine-readable format, as derived from agency policy.
	Guidance: Agency-derived machine-readable policies that are expected to be implemented by the TRUST capability include, for example, requirements for clearances, background checks, and non-disclosure agreements. This is the PAP (See CDM AV-2) that establishes the desired state information that will be compared with actual state at the PDP.
Collect TRUST information from authoritative sources	
TRUST-2-1	The TRUST capability shall collect TRUST attributes on in-scope users from Agency authoritative sources.
	Guidance: Specific attributes for TRUST are included in the CDM DMD. An Agency authoritative source is an Agency-designated source that has correct and current information regarding user TRUST attributes. For example, an Agency Human Resources (HR) system may be the authoritative source of information about Agency employees (e.g., name, employee ID, organizational unit, job title, home address, date of birth, supervisor/manager). This is the actual state for the PDP.
Compare Agency actual state to TRUST policy	
TRUST-3-1	The TRUST capability shall identify a defect when an in-scope user does not meet the Agency-defined TRUST policy.
	Guidance: This is the PDP where the actual state is compared with the desired state policy to identify defects. The specific defect checks are detailed in the CDM DMD, and include, for example, expired trust. An in-scope user is defined as government employees or contractors in possession of a PIV card.
Display TRUST information and generate reports locally	
TRUST-4-1	The TRUST capability shall report collected TRUST attributes locally through the following methods, as requested by the administrator: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)
	Guidance: Reporting locally means that the information can be displayed on a tool display, sent to a printer, or output to a document.

Req. UID	Requirement Text
TRUST-4-2	The TRUST capability shall report TRUST defects locally through the following methods, as requested by the administrator: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)
	Guidance: Reporting locally means that the information can be displayed on a tool display, sent to a printer, or output to a document.
Report TRUST information to Agency dashboard	
TRUST-5-1	The TRUST capability shall report collected TRUST attributes for each in-scope user.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported attributes are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).
TRUST-5-2	The TRUST capability shall report TRUST defects for each in-scope user.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported defects are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).

2.3.2 BEHAVE Capability

The CDM BEHAVE capability ensures that an authorized user exhibit the appropriate behavior for their role. For CDM, appropriate security-related behavior is defined as actions that have been explained, and "agreed to" by the user via user agreements, training, job requirements, or similar methods. This capability provides an Agency with insight into risks associated with non-conformance with policies for accessing systems and data by authorized users. The BEHAVE capability will apply only to in-scope users (employees and contractors, who will each have a PIV card).

Poorly trained users can unknowingly engage in behaviors that compromise systems, expose sensitive data, or subvert policies meant to mitigate risk. This capability is dependent on the existence of a set of attributes that denote roles or characteristics that require specific security-related behaviors per policy. All authorized users have minimum security-related training requirements. Authorized users with special access may have additional training requirements. Agencies determine the general security training (e.g., annual cybersecurity training) required for all users and additional specialized security training for some users depending on their assigned responsibilities.

The following are the functions of the BEHAVE capability:

- **Establish Agency BEHAVE desired state in machine-readable policies** stores the Agency-defined desired-state BEHAVE policies in machine-readable form. BEHAVE maintains the desired state.
- **Collect BEHAVE information from authoritative sources** collects actual state information from the BEHAVE capability authoritative sources which are existing systems that vary by Agency. These contain attributes regarding training and any related certifications expiration date, etc.
- **Compare Agency actual state to BEHAVE policy** compares Agency desired state with collected actual state and identifies defects. This is the PDP.
- **Display BEHAVE information and generate reports locally** provides the administrator the ability to display BEHAVE information and generate reports.
- **Report BEHAVE information to Agency dashboard** reports BEHAVE information and BEHAVE defects to the Agency Dashboard.

The BEHAVE capability must integrate with external systems that are authoritative sources of actual state information such as:

- Learning management systems or equivalent

Properly implemented and acted upon, the BEHAVE capability helps to ensure that every user has received appropriate and up-to-date training and knowledge/certification for access to sensitive systems and information.

2.3.2.1 BEHAVE Functional Requirements

This section provides functional requirements for the BEHAVE capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 11. BEHAVE Functional Requirements

Req. UID	Requirement Text
Establish Agency BEHAVE desired state in machine-readable policies	
BEHAVE-1-1	The BEHAVE capability shall implement BEHAVE policies in machine-readable format, as derived from agency policy.
	Guidance: Agency-derived machine-readable policies that are expected to be implemented by the BEHAVE capability include, for example, training completion dates, and certification dates. This is the PAP that establishes the desired state information that will be compared with actual state at the PDP.
Collect BEHAVE information from authoritative sources	
BEHAVE-2-1	The BEHAVE capability shall collect BEHAVE attributes on in-scope users from Agency authoritative sources.
	Guidance: Specific attributes for BEHAVE are included in the CDM DMD. An Agency authoritative source is an Agency-designated source that has correct and current information regarding user BEHAVE attributes. For example, an Agency training system may be the authoritative source of information about Agency employees (e.g., name, employee ID, organizational unit, system training dates, certification dates) and captures specific BEHAVE information that is unique to agencies, based on an agency's policy regarding specific roles (e.g., specialized training for domain administrators). This is the actual state for the PDP. In-scope users are defined as employees and contractors who have a PIV card.
Compare Agency actual state to BEHAVE policy	
BEHAVE-3-1	The BEHAVE capability shall identify a defect when an in-scope user does not meet the Agency-defined BEHAVE policy.
	Guidance: This is the PDP where the actual state is compared with the desired state policy to identify defects. The specific defect checks are detailed in the CDM DMD and include, for example, expired training or certification dates, or that users training is sufficient to their assigned role.
Display BEHAVE information and generate reports locally	
BEHAVE-4-1	The BEHAVE capability shall report collected BEHAVE attributes locally through the following methods, as requested by the administrator: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)
	Guidance: Reporting locally means that the information can be displayed on a tool display, sent to a printer, or output to a document.
BEHAVE-4-2	The BEHAVE capability shall report BEHAVE defects locally through the following methods, as requested by the administrator: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)

Req. UID	Requirement Text
	Guidance: Reporting locally means that the information can be displayed on a tool display, sent to a printer, or output to a document.
Report BEHAVE information to Agency dashboard	
BEHAVE-5-1	The BEHAVE capability shall report collected BEHAVE attributes for each in-scope user.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported attributes are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).
BEHAVE-5-2	The BEHAVE capability shall report BEHAVE defects for each in-scope user
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported defects are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).

2.3.3 CRED Capability

The CDM CRED (credentials and authenticators) capability ensures that account credentials are assigned to, and are used only by, authorized users or services to access agency systems, services, and facilities. CRED binds a type of credential or authenticator to an identity established in TRUST with a level of assurance and is used to grant logical access. The CRED capability will apply only to in-scope users (employees and contractors, who will each have a PIV card). In-scope users have network accounts, where the primary control mechanism for network authentication is the Agency's Microsoft Active Directory Implementation.

The CRED capability provides an Agency with insight into risks related to weaknesses in its credential management. The CRED capability collects data associated with the credentials issued to a user (i.e., CRED attributes) including the credential type and dates of issuance, review, and renewal.

CRED capability will help ensure that every user can be authenticated appropriately for access to sensitive systems and information. The capability will also provide insight into whether authentication, reissuance, and revocation policies are following policy specified by the Agency.

The following are the functions of the CRED capability:

- **Establish Agency CRED desired state in machine-readable policies** stores the Agency-defined desired-state CRED policies in machine-readable form. CRED maintains the desired state.
- **Collect CRED information from authoritative sources** collects actual state information from the CRED capability authoritative sources which are existing systems that vary by Agency. These contain attributes regarding credentials for users that enable access to Agency systems and networks.
- **Compare Agency actual state to CRED policy** compares Agency desired state with collected actual state and identifies defects. This is the PDP.
- **Display CRED information and generate reports locally** provides the administrator the ability to display CRED information and generate reports.
- **Report CRED information to Agency dashboard** reports CRED information and CRED defects to the Agency Dashboard.

The CRED capability is expected to integrate with external systems that are authoritative sources of actual state information such as:

- Identity Management System (IDMS) for PIV card issuance

An Agency authoritative source is an Agency designated source that has correct and current information regarding user CRED attributes. For example, an Agency authorization system may be the authoritative source of information about Agency employees (e.g., X.509 certificates, user identities, and public/private key pairs, PIV cards or other token issuance systems).

While the PIV card is the preferred authenticator for use in the Federal government, there are times when the use of PIV is not possible.

The following is a non-exclusive list of tool functionalities that support CRED capability:

Tool Category Name	Summary of Functionality
Public Key Infrastructure (PKI) tools	Tools to establish and manage public key encryption, and help to authenticate the identity of communicating parties or devices
Identity and Access Management tools	Tools to identify and confirm users, applications, and devices. These will grant appropriate authorities and permissions. They can also establish and enforce policies and procedures that apply to user groups to include roles and responsibilities
Access certification tools	Enables managers or system owners to review users' entitlements (access) to a system to ensure that the users have access to only what they need
Authentication mechanisms	Tools that authenticate the user with a specific challenge or authentication technology, such as user name and password or one-time passwords to allow access to protected resources
Audit reporting tools	Enables evaluation of the company's compliance with regulations, as well as measuring their performance against an established set of criteria. These are done to identify security problems and gaps, establish a security baseline, compliance with internal and external policies and requirements, and determine if security training is adequate

2.3.3.1 CRED Functional Requirements

This section provides functional requirements for the CRED capability. The “shall” statements included in this set of requirements often require agency policy inputs to accurately develop machine readable policies (i.e., tool configurations) that facilitate a true representation of an agency’s desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 12. CRED Functional Requirements

Req. UID	Requirement Text
Establish Agency CRED desired state in machine-readable policies	
CRED-1-1	The CRED capability shall implement CRED policies in machine-readable format, as derived from agency policy.
	Guidance: Agency-derived machine-readable policies that are expected to be implemented by the CRED capability include, for example, the review period for credentials. This is the PAP that establishes the desired state information that will be compared with actual state at the PDP.
Collect CRED information from authoritative sources	
CRED-2-1	The CRED capability shall collect CRED attributes on in-scope accounts and users from Agency authoritative sources.
	Guidance: Specific attributes for CRED are included in the CDM DMD. This is the actual state for the PDP. In-scope users are defined as employees and contractors who have a PIV card.
Compare Agency actual state to CRED policy	
CRED-3-1	The CRED capability shall identify a defect when an in-scope account or user credential does not meet the Agency-defined CRED policy.
	Guidance: This is the PDP where the actual state is compared with the desired state policy to identify defects. The specific defect checks are detailed in the CDM DMD, and include, for example, expired credentials or credentials that have not been reviewed.

Req. UID	Requirement Text
Display CRED information and generate reports locally	
CRED-4-1	The CRED capability shall report collected CRED attributes locally through one or more of the following methods: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)
	Guidance: Reporting locally means that the information can be displayed on a tool display, sent to a printer, or output to a document.
CRED-4-2	The CRED capability shall report CRED defects locally through one or more of the following methods: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)
	Guidance: Reporting locally means that the information can be displayed on a tool display and also sent to a printer.
Report CRED information to Agency dashboard	
CRED-5-1	The CRED capability shall report collected CRED attributes for each in-scope user.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported attributes are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).
CRED-5-2	The CRED capability shall report CRED defects for each in-scope user.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported defects are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).

2.3.4 PRIV Capability

The CDM PRIV capability provides the agency with insight into risks associated with authorized users being granted excessive privileges to systems and information at any level of sensitivity. The purpose of the capability is to ensure that privileges for logical access are assigned to authorized people or accounts that require authorized access for job functions. This capability is dependent on the existence of a set of attributes that denote roles or characteristics that require or restrict specific privileges per policy. Non-person entities are not covered by PRIV. The PRIV capability will apply only to in-scope users (employees and contractors, who will each have a PIV card) and associated accounts.

PRIV identifies instances in which agency policy, related to in-scope privileged user accounts, is not being followed. In addition, PRIV also offers ILM and PAM as sub-capabilities. ILM is designed to enhance an agency's ability for managing privileged user accounts while PAM implements more rigorous authentication and authorization methods for privileged users.

Note: Privileged user accounts have "elevated" or "administrator-like" privileges that are above the normative baseline defined for an unprivileged user. The Agencies will define the level of access that defines privileged users.

Agencies develop policies for privileges and entitlements and reflect them in the desired state attribute values. The PRIV capability collects the actual state privileges and entitlement attributes for all privileged and unprivileged accounts from authoritative sources, including:

- Active Directory or other systems using Agency Enterprise Lightweight Directory Access Protocol (LDAP)

Note: Entitlements are defined as specific rights that are traceable to a higher-level privilege. For example, an account that is given Network Administrator privileges may also inherit entitlements that cover firewalls and routers. Attributes include, for example, the type and a description of the entitlement.[27]

PRIV compares the Agency policy reflected by the desired state with the collected actual state attribute values from authoritative sources to identify defects in a PDP. The PAM sub-capability provides a PEP for privileged user access management, primarily for administrators who have "root" or administrator" access on Linux and Windows systems, respectively. The PEP will make privileged user access decisions.

CDM has narrowed the scope of the PAM sub-capability to focus on the most critical human and system assets. In-scope users include Agency employees and contractors who have been issued valid PIV cards and have highly elevated privileges on Agency systems. Additionally, workstations that are used to perform administration on systems that have infrastructure impact (i.e., broad impact to the systems operating on an Agency network) are also in-scope of the PAM sub-capability due to the sensitive access these assets have. The PRIV ILM and PAM sub-capabilities secure devices or systems that have infrastructure impact and include the following:

- Workstation (dedicated management endpoints for administration of IT infrastructure
- Servers
- Mainframes
- Network devices
- Mobile Device Manager (MDM)/ Enterprise Mobility Management (EMM) (administer mobile devices)

The following are the PRIV functions:

- **Establish Agency PRIV desired state in machine-readable policies** stores the Agency-defined desired-state PRIV policies in machine-readable form. PRIV maintains the desired state and logs changes.
- **Collect PRIV information from authoritative sources** collects actual state information from the PRIV capability authoritative sources which are existing systems that vary by Agency. These contain attributes regarding privilege expiration date, etc. PRIV logs all collected data.
- **Compare Agency actual state to PRIV policy** compares Agency desired state with collected actual state and identifies defects. This is the PDP. PRIV logs all defects identified.
- **Display PRIV information and generate reports locally** provides the administrator the ability to display PRIV information and generate reports. The PRIV logs can be exported to SIEM tools.
- **Report PRIV information to Agency dashboard** reports PRIV information and PRIV defects to the Agency Dashboard.

PRIV has two sub-capabilities: ILM and PAM.

[27] CDM Data Model Document, Version 3.8.1, 6 March 2020.

The following is a non-exclusive list of general tool functionalities that support PRIV functional requirements:

Tool Category Name	Summary of Functionality
Identity and access management tools	Tools to identify and confirm users, applications, and devices. These will grant appropriate authorities and permissions. They can also establish and enforce policies and procedures that apply to user groups to include roles and responsibilities
Privileged account management tools	Enables the control and monitoring of privileged users activities, including access to business systems and their functionality once logged in, ensuring the resources are secure
Credential management tools	Maintains the credential and associated support over the lifecycle, common processes include renewal, reissuance, suspension, blocking, unblocking, and revocation
Compliance verification tools	Tools to assist in the monitoring and assessment of systems to ensure they comply with industry and security standards, as well as corporate and regulatory policies and requirements, helping to identify systems that are non-compliant

2.3.4.1 PRIV Functional Requirements

This section provides functional requirements for the PRIV capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 13. PRIV Functional Requirements

Req. UID	Requirement Text
Establish Agency PRIV desired state in machine-readable policies	
PRIV-1-1	The PRIV capability shall implement PRIV policies in machine-readable format, as derived from agency policy.
	Guidance: Agency-derived machine-readable policies that are expected to be implemented by the PRIV capability include, for example, rules for number of privileged users, privilege expiration time, required privilege review time period, account status, etc. This is the PAP that establishes the desired state information that will be compared with actual state at the PDP.
Collect PRIV information from authoritative sources	
PRIV-2-1	The PRIV capability shall collect PRIV and entitlement attributes on in-scope privileged accounts from Agency authoritative sources.
	Guidance: Specific attributes for PRIV are included in the CDM DMD, and include, for example, privilege type, privilege status, and review date. This is the actual state for the PDP. In-scope privileged accounts are employees and contractors, who will each have a PIV card.
Compare Agency actual state to PRIV policy	
PRIV-3-1	The PRIV capability shall identify a defect when the PRIV or entitlements for an in-scope privileged account do not meet the Agency-defined PRIV policy.
	Guidance: This is the PDP where the actual state is compared with the desired state policy to identify defects. The specific defect checks are detailed in the CDM DMD, and include, for example, expired PRIV. See the CDM DMD for the list of defect checks performed.
PRIV-3-2	The PRIV capability shall log events relating to any of the following activities: • Authentication events to the PRIV capability console • Authorization events regarding access/privileges to the PRIV capability • Changes to the Agency-defined PRIV policy
	Guidance: The intent of this requirement is to support an ability to audit administrative-type actions in the PRIV tool/technologies, including login attempts, logoffs, adding additional users/permissions in the PRIV tool, and changing the configurations.

Req. UID	Requirement Text
Display PRIV information and generate reports locally	
PRIV-4-1	The PRIV capability shall report collected PRIV attributes locally through the following methods, as requested by the administrator: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)
	Guidance: Reporting locally means that the information can be displayed on a tool display, sent to a printer, or output to a document.
PRIV-4-2	The PRIV capability shall report PRIV defects locally through the following methods, as requested by the administrator: • Tool/sensor console • Send report to printer (hard copy) • Export to a document/file (soft copy)
PRIV-4-3	The PRIV capability shall integrate with SIEM systems to export logs, per Agency policy.
	Guidance: The intent is to integrate the PRIV capability with existing agency SIEM platforms that are operational.
Report PRIV information to Agency dashboard	
PRIV-5-1	The PRIV capability shall report collected PRIV attributes for each in-scope user.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported attributes are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).
PRIV-5-2	The PRIV capability shall report PRIV defects for each in-scope user.
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Reported defects are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards).

2.3.4.1.1 Identity Lifecycle Management Sub-Capability

CDM ILM, a sub-capability under the PRIV capability, enables automation throughout the IdAM lifecycle by adjusting information in connected repositories to address changing user positions and responsibilities. This includes adding and removing entitlements (authorization to access) to systems, roles, and accounts based upon rules that specify the intent (desired state) of the Agency. ILM automates provisioning and matching system privileges with the responsibilities of a user's current role. These changes are monitored and logged. ILM notifies those responsible for reviewing and validating user's privileges, to ensure users still retain the proper privileges.

ILM also prompts managers and other responsible parties to review TRUST, BEHAVE, CRED, and PRIV attributes such as background investigations, training, system credentials and privileges. The review process can identify, for example, missing training and unnecessary excess privileges. These repositories of user roles and permissions may be centrally located in an Agency, in order to maintain and update user accounts as needed.

The following are the ILM functions:

1. **Manage workflow of user access permissions** notifies the administrators and reviewers when changes to user accesses have been made, or require approval, and enforces approval policy
2. **Provision user accounts and entitlements** provisions in-scope privileged user accounts and entitlements, providing only privileges necessary to perform their specific role within the agency.
3. **Establish Agency ILM desired state in machine-readable policies** captures the policies needed for ILM functionality, derived from agency policies.

The following is a non-exclusive list of general tool functionalities that support ILM functional requirements:

Tool Category Name	Summary of Functionality
IdAM Identity Lifecycle Management tools	Tools and processes to keep identities accurate and synchronized across systems, which include provisioning apps and managing user attributes and entitlements

2.3.4.1.1.1 ILM Functional Requirements

This section provides functional requirements for the ILM capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 14. ILM Functional Requirements

Req. UID	Requirement Text
Manage workflow and user access permissions	
ILM-1-1	The ILM capability shall prompt the agency-delegated authorized reviewer to review in-scope privileged user privileges and entitlements when they have not been reviewed in the Agency defined maximum review period time.
	Guidance: The Agency should review and validate that privileges are still needed on a periodic basis as defined in Agency policy.
ILM-1-2	The ILM capability shall integrate with Agency authoritative source systems to enforce Agency policy-related changes for in-scope privileged users whose PRIV information necessitates PRIV-related updates
	Guidance: This is a workflow that integrates maintaining attributes and provisioning users for system access. Privileged user information changes could include TRUST, BEHAVE, CRED, or PRIV attributes. Changes could also result from personnel actions including hiring or departure.
ILM-1-3	The ILM capability shall notify Agency authoritative source systems when changes to the in-scope privileged user information necessitates PRIV-related updates, per Agency policy.
ILM-1-4	The ILM capability shall enforce approvals of privileged user changes using an organizational hierarchy.
	Guidance: Each agency will have an organizational structure for approval of privileged user changes. This establishes the organizational hierarchy for approvals in ILM functions. Some implementation examples of organizational delegation include Active Directory OUs, Microsoft Global Access Lists organizational hierarchies (e.g., reports to, managed by, etc.).
ILM-1-5	When configured by the administrator, the ILM capability shall delegate administrative responsibilities of the ILM capability from one authorized administrator to another, based on Agency policy.
	Guidance: An organization hierarchy for ILM functions must be established to support this. Administrative responsibilities include provisioning, reviewing privileges, etc.
ILM-1-6	The ILM sub-capability shall log each workflow event.
	Guidance: Any changes in user access permissions made as part of the workflow associated with ILM are logged.
ILM-1-7	When integrated with other IdAM authoritative sources or platforms to automate the user provisioning/deprovisioning process based on Agency policy, The ILM sub-capability shall exchange information via IdAM-related industry standards
	Guidance: IdAM-related standards include, but is not limited, to System for Cross-Domain Identity Management (SCIM). See ILM-1-2, ILM-1-3, ILM-1-4 for more information on automating the user provisioning/deprovisioning process.
ILM-1-8	The ILM capability shall provide a web-based graphical user interface for administrative functions.
Provision user accounts and entitlements	

Req. UID	Requirement Text
ILM-2-1	When configured by the administrator, the ILM capability shall automatically provision in-scope privileged user accounts and entitlements to Agency authoritative privilege repositories, upon the occurrence of a workflow event identified in Agency policy.
	Guidance: An agency may or may not have policy that allows for automatic provisioning. Workflow events could include a new hire, departure, or change in job function. Privilege repositories are centralized directories or administration points which may control accesses/privileges, such as Microsoft Active Directory.
ILM-2-2	Upon input from the administrator, the ILM capability shall provision in-scope privileged user accounts and entitlements to Agency authoritative privilege repositories.
	Privilege repositories are centralized directories or administration points which may control accesses/privileges, such as Microsoft Active Directory.
ILM-2-3	The ILM capability shall provision only privileges necessary for the user's role, per Agency policy.
	Guidance: The Agency may limit privileges based on assigned role. These limitations would be defined in the Agency policy/desired state.
ILM-2-4	The ILM capability shall provision privileges and entitlements based on Agency specified attribute criteria.
	Guidance: The agency specified criteria could include the group the user is assigned to, user responsibilities, etc. See ILM-1-2, ILM-1-3, ILM-1-4 for additional information.
ILM-2-5	The ILM capability shall log each provisioning event.
Establish Agency ILM desired state in machine-readable policies	
ILM-3-1	The ILM capability shall implement ILM policies in machine-readable format, as derived from agency policy.
	Guidance: These policies govern management of privileged user accounts to protected resources.

2.3.4.1.2 Privileged Access Management Sub-Capability

CDM PAM, a sub-capability under PRIV, focuses on the most critical human and system assets. In-scope users include Agency employees and contractors who have been issued valid PIV cards and have highly elevated privileges on Agency systems. The PAM sub-capability provides a PEP for privileged user access management, primarily for administrators who have "root" or administrator" access on Linux and Windows systems, respectively. The PEP will authenticate privileged users and make access decisions. Typically these decisions are made via the user's PIV card, however in some cases where a PIV card cannot be implemented, Agencies may use a vault that uses a PIV card for authentication to enable a session between the vault tool and a target device that has no native ability to accept PIV cards.

The PAM sub-capability will also protect agency systems and networks, by allowing only authorized user's access as a privileged user, and will also monitor their activities. Other safeguards include strong credentialing, such as AAL3, or other cryptographic security to ensure target devices are protected.

The following are the PAM functions:

1. **Authenticate user access** authenticates in-scope privileged users for access to target devices.
2. **Authorize user access** provides privileged users access to agency-defined target devices.
3. **Validate PRIV accounts** determines if all active and inactive privileged user accounts are correctly identified within the agency.
4. **Establish Agency PAM desired state in machine-readable policies** captures the policies that address access to protected resources.

The following is a non-exclusive list of general tool functionalities that support PAM functional requirements:

Tool Category Name	Summary of Functionality
Privileged account management tools	Enables the control and monitoring of privileged users activities, including access to business systems and their functionality once logged in, ensuring the resources are secure

2.3.4.1.2.1 PAM Functional Requirements

This section provides functional requirements for the PAM sub-capability. The "shall" statements included in this set of requirements often require agency policy inputs to accurately develop machine readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 15. PAM Functional Requirements

Req. UID	Requirement Text
Authenticate user access	
PAM-1-1	The PAM capability shall authenticate in-scope privileged users using a PIV-based strong authenticator.
	Guidance: This is the PEP where a privileged user is authenticated.
PAM-1-2	The PAM capability shall authenticate in-scope privileged users using a secrets vault for target devices that cannot accept PIV authenticators directly.
	Guidance: Based on Agency policy, an Agency may use a Vault that uses a PIV card for authentication to enable a session between the vault tool and a target device that has no native ability to accept PIV cards. A "secrets vault" is a trusted, secured repository of strong passwords ("secrets") which are valid for authenticating to target devices.
PAM-1-3	The PAM capability shall maintain secrets based on random number generators or hashing functions generated and stored in a Federal Information Processing Standards (FIPS) 140-2 or 140-3 compliant cryptographic modules.
	Guidance: "Maintain" generically refers to the functionality to generate and securely store secrets. The PAM capability will generate secrets that are used to log into the targets, in accordance with the correct standards. It then stores the key in a FIPS-validated module. The PAM tool may utilize secrets within a "secrets vault" to broker access to a resource and/or support assertion models. Secrets can be changed at short time-based intervals and can include cryptographic asymmetric key exchanges to enable strong (e.g., PIV) authentication for privileged accounts that do not natively support PIV authentication.
PAM-1-4	The PAM capability shall be able to change secrets at short time-based intervals (minutes) and after each use in accordance with Agency policy and performance capabilities.
PAM-1-5	The PAM capability shall log each authentication event.
Authorize user access	
PAM-2-1	The PAM capability shall grant privileged users access to agency-defined target devices for which they hold privileges and entitlements, per Agency policy.
	Guidance: This is the PEP where a privileged user is provided access, if the appropriate privileges and entitlements are held, and rejected access if not.
PAM-2-2	The PAM capability shall grant privileged users access to agency-defined target devices for which they hold privileges and entitlements and comply with TRUST, BEHAVE, and CRED attributes, per Agency policy.
	Guidance: Some agencies may perform compliance checks on clearance/suitability, training, and credential information before granting access.
PAM-2-3	The PAM capability shall only grant administrative access to the PAM console to authorized in-scope privileged users with the proper strong credentials, using hardware-based authenticators.
	Guidance: The intent is to require strong authentication using multiple factors (something you have, something you know). PIV cards satisfy this requirement.

Req. UID	Requirement Text
PAM-2-4	If strong encryption is required, per agency policy, the PAM capability shall utilize FIPS 140-2 or FIPS 140-3 validated cryptography to protect the sessions with agency-defined target devices.
	Guidance: This could be asymmetric key exchanges (e.g., SSH, secure RDP), etc.
PAM-2-5	The PAM capability shall employ a jump box to broker privileged account access to a target device, based on Agency policy.
	Guidance: Some Agencies may require a jump box (a system connected to two networks in separate security zones, providing a means of access between them) to be the only system allowed to provide a connection between the systems.
PAM-2-6	The PAM capability shall prohibit privileged users from accessing stored secrets, based on Agency policy.
	Guidance: The PRIV capability manages privileged account sessions by securely controlling secrets that are exchanged among the target resource, the session manager, and the secrets vault. It is preferred that the user cannot see the stored secret, the system simply supplies it. However, some agencies may have policies that allow privileged users to copy and paste the secrets.
PAM-2-7	The PAM capability shall log each privileged user access event.
	Guidance: Privileged user access events include for example, logging into/out of the PAM capability and also logging into/out of an endpoint.
PAM-2-8	Upon administrator command, the PAM capability shall provide access to the target device through industry standard remote access protocols that protect data in transit, per Agency policy
	Guidance: These protocols include, but are not limited to, Remote Desktop Protocol (RDP) or Secure Shell (SSH) services.
Validate PRIV accounts	
PAM-3-1	The PAM capability shall discover privileged accounts on the network.
	Guidance: Discover all active and inactive accounts, including emergency accounts and set up accounts. The collection of this information is a CDM requirement. The use of the information is up to the Agency. This actual state information collected from the network can be compared with actual state from Agency authoritative sources to validate the authoritative sources, either manually by the Agency or using a tool.
PAM-3-2	The PAM capability shall maintain an updated inventory of privileged accounts discovered on the network.
	Guidance: The PAM capability is intended to serve as a source of PRIV information for the CDM system (in conjunction with other authoritative sources such as Active Directory, etc.)
Establish Agency PAM desired state in machine-readable policies	
PAM-4-1	The PAM capability shall implement PAM policies in machine-readable format, as derived from agency policy.
	Guidance: These policies govern access to protected resources with access managed by PAM.

2.4 Network Security Management (NSM) Capability Area

The Network Security Management (NSM) Capability Area builds on the CDM capabilities provided by Asset Management and Identity and Access Management. The NSM capabilities include network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. NSM capabilities move beyond asset management to a more extensive and dynamic monitoring of security controls. This includes preparing for and responding to behavior incidents, ensuring that software/system quality is integrated into the network/infrastructure, detecting internal actions and behaviors to determine who is doing what, and finally, mitigating security incidents to prevent propagation throughout the network/infrastructure.

NSM is broken into four capabilities. These capabilities are briefly summarized below, and the detailed requirements are separately specified later in the BOUND, MNGEVT, OMI, and DBS sections.

- **BOUND** (Section 2.4.1) describes how the network is protected through filtering, network access control, and encryption.
- **MNGEVT** (Section 2.4.2) describes ongoing assessment, preparing for events/incidents, audit data collection from appropriate sources, and identifying incidents through the analysis of data.
- **OMI** (Section 2.4.3) describes ongoing authorization, audit data aggregation/correlation and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).
- **DBS** (Section 2.4.4) describes preventing exploitable vulnerabilities from being effective in the software/system while the software/system is in development or deployment.

The iterative and continuous interaction between MNGEVT ongoing assessment and OMI Ongoing Authorization capabilities provides a systematic approach to prepare, detect, respond to, and recover from existing residual security risk and newly discovered security risk in near-real time. This automated approach is an attempt to move away from the traditional, static, multi-year risk assessment and authorization process that is slow to respond to security risks, attacks, and compromises.

2.4.1 Manage BOUND, or "How is the network protected?"

Managing network protection requires capabilities that limit, prevent, and/or allow the removal of unauthorized network connections and access. Such access would allow attackers to cross internal and external network boundaries and then pivot to gain deeper network access and/or capture network resident data at rest or in transit.

This capability includes the use of devices such as firewalls that sit at a boundary and regulate the flow of network traffic. It also includes the use of encryption to protect traffic that must cross logical boundaries. It also includes Network Access Control to ensure that a device can only connect to an enterprise network if the device is explicitly authorized to connect, and is compliant with the stated hardware, software, configuration, and patching policies.

BOUND is categorized into three security sub-capabilities:

- BOUND-F to Manage Network Filters and Boundary Controls
- Network Access Control (NAC) to control access to the network
- BOUND-E to Monitor and Manage Cryptographic Mechanisms Controls

2.4.1.1 BOUND-F Requirements

Manage Network Filters and Boundary Controls (BOUND-F) network filters include devices such as firewalls and gateways that sit at the boundary between enclaves (such as a trusted internal network or subnet and an external or internal, less trusted network). The filters apply sets of rules and heuristics to regulate the flow of traffic between the trusted and less trusted sides of the boundary. The filters can also monitor tags related to information at any sensitivity level, such as PII, to ensure transmission (e.g., sharing) is restricted to authorized locations, and authorized recipients/third parties.

The BOUND-F capability is further divided into the following categories:

- Content Filtering
- Packet Filtering
- Layer 2 Filtering
- Encapsulation Filtering

BOUND-F reduces the probability that unauthorized traffic will pass through a network boundary. This includes the requirement that the boundary filtering policies are monitored, reviewed, and reauthorized per Agency policy. Network boundary security focuses on network weaknesses and vulnerabilities that can affect the network's ability to prevent the disclosure of confidential data, to determine when the integrity of the network is compromised, and to detect when malicious behavior impacts the network's availability. For the purposes of BOUND-F, network encryption points (e.g., virtual private networks) are considered network boundaries. Policies involving network encryption will have attributes associated with both BOUND-F and BOUND-E. A BOUND-F device must be capable of filtering (actively or passively) network traffic at some level per policy established by the Agency.

The BOUND-F capability provides Agencies visibility into the risk associated with boundary filtering policies, to include the use of network encryption. BOUND-F traffic filtering policies can be applied at one or more layers of the network stack. Policies at layers 4 and above typically filter based on specific applications and application content (e.g., filtering email messages and messages containing spam, malware, sensitive and PII data). Those policies would contain content filtering records that describe the content that was filtered based on rules and policies.

Collecting data associated with the boundary filtering policy and the filtering policy required for network flow across a boundary provides measurable data elements for the creation of automated security checks. These security checks provide the basis for automating the monitoring, reporting, and prioritizing of boundary filtering policy deficiencies, including those specific to sensitive information within an Agency's cyber environment. Through CDM, deficiencies are displayed for review and action.

BOUND-F helps to ensure that the filtering policies for enclaves and systems are properly implemented to secure network traffic crossing boundaries. The capability also provides insight into duplicative and/or conflicting filtering policies.

2.4.1.1.1 BOUND-F Operational Requirements

BOUND_OR-1-1: Shall enforce one or more filtering policies using one or more PDPs and one or more PEPs. These filtering policies control what data can enter or exit the system and may consist of one or more of the following filter types:

a. Content filtering to filter traffic based on the application content of the traffic, including both the syntax and the semantic content. For example, policies at layers 4 and above typically filter based on specific applications and application content (e.g., filtering email messages and messages containing spam and/or malware). Those policies describe the content that is filtered based on rules and policies.
b. Packet filtering to filter traffic based on IP packet header information and optionally on other IP datagram externals such as datagram length or frequency. For example, policies at the IP layer typically filter based on IP packet header information (e.g., filtering based on source and destination IP address). Those policies describe the datagrams and/or sessions that are filtered based on rules and policies.
c. Layer 2 filtering to filter traffic based on layer 2 header information and optionally based on other layer 2 traffic externals, such as length or frequency. For example, policies at the data link layer (layer 2) typically filter based on layer 2 header information (e.g., filtering based on source and destination Ethernet address or virtual local area network number). Those policies describe the packets that are filtered based on rules and policies.
d. Encapsulation filtering to filter traffic based on the encapsulation method and traffic characteristics (e.g., IP header attributes, application, and packet content). For example, encapsulation policies describe how data from one network protocol is translated into another network protocol so that the data can continue to flow across the network (e.g., encrypting traffic between two IP subnets across a wide area network). Those policies describe the network flows that are encapsulated and filtered based on rules and policies.
e. Boundary filtering (a combination of multiple filtering capabilities) based on the policies and traffic characteristics. For example, boundary policies combine multiple filtering

policies (e.g., IP layer and content filtering) into the overall policy for filtering traffic across a boundary (and may be implemented on one or more devices).

2.4.1.1.2 BOUND-F Functional Requirements

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers, the MDR (e.g., device categorization, filtering policies), the MUR (e.g., physical security training), and the Master System Record (MSR) (e.g., boundary/interconnection between systems and the associated boundary filtering policies). This capability is related to PRIV, TRUST, CRED, and BEHAVE to support logical access control decisions for access to systems, and information at any level of sensitivity. This capability is related to DATA_DLP and DATA_PROT when content filtering is used to enforce data protection policies.

BOUND_FR-1-1: Shall collect and report information related to the implementation of filtering policies at one or more levels in the protocol stack. This information support the enforcement of filtering policies. Information collected and reported on may consist of one or more of the following types:

a. Content filtering that directly filters traffic based on the application and application content. For example, the content is based on concepts understood at the application layer. Content filtering is described in terms of the applications (and the application characteristics) on which filtering can occur (e.g., URL filtering for HTTP content) and whether a proxy or translation is performed.
b. IP layer (packet) filtering that filters traffic based on the contents of IP layer protocols. Packet filtering is described in terms of what portions of the IP header are being used for the filtering decision and whether proxying or translation is being performed.
c. Layer 2 filtering that filters traffic at the data link layer, or layer 2, in the protocol stack. Layer 2 filtering is described in terms of which layer 2 protocol and what aspects of the protocol are being used for the filtering decision.
d. Encapsulation filtering that shows how data from one network protocol is translated into another network protocol so that the data can continue to flow across the network. Encapsulation filtering is described in terms of the encapsulation method and the traffic characteristics (e.g., IP header attributes, application, and packet content).
e. Boundary filtering of policies to determine what traffic can flow, and what traffic is blocked across a boundary. A boundary filtering policy is of the set of filtering policies for a boundary, including metadata about that policy.

2.4.1.1.3 BOUND-F Tool Functionalities

The following is a non-exclusive list of tool functionalities that support BOUND-F capability:

- Forward Web Proxies (or Secure Web Gateways)
- Reverse Web Proxies
- Web Application Firewalls
- Application Aware Firewalls (or Next Generation Firewalls)
- Email Security Gateways (or Secure Email Gateways)
- Database Firewalls
- Intrusion Detection or Prevention Systems

2.4.1.2 NAC Requirements

NAC ensures that a device can connect to an agency network only if the device is authorized to connect and is compliant with the agency's stated hardware and software configuration and patching policies, thereby reducing the network attack surface. NAC checks the security posture (compliance with agency policy) of devices requesting to connect and provides the PEP for granting those devices access. The agency policy may simply permit or block (deny) network access or may be more complex and allow for placing a device into quarantine and forcing patching or upgrading of the device to become policy compliant, before allowing network connection. NAC also logs events (devices allowed access, devices quarantined, etc.) and provides alerts to agency personnel, based on agency policy. Finally, NAC information is provided to the agency dashboard.

Devices are authorized to connect if they appear in the agency's hardware inventory as authorized, and comply with agency policy on hardware and software, configuration, and patching.

The NAC capability covers wired and wireless device connection attempts, depending upon agency policy. Mobile connections are covered by the CDM Enterprise Mobility Management (EMM) capability in the Asset Management Capability Area. NAC is a CDM Bound sub-capability in the Network Security Management Capability Area and is associated with the PROTECT function as described in the NIST CSF. NAC requires a mature HWAM capability and may integrate with the IdAM and other capabilities. HWAM provides information on hardware discovered on the network.

NAC is expected to integrate with external systems such as SIEM systems, service desk automated ticketing and tracking systems, configuration management database (CMDB) management, vulnerability management systems, automated patching systems, and current networking infrastructure, based on Agency policy.

The following are the eight CDM NAC functions:

1. **Represent and Enforce Desired State for NAC in Machine-Readable Policy** implements sufficiently mature agency Access Control and other relevant policies and procedure sets into a machine-readable form to serve as the foundation for the PEP within the CDM system.
2. **Detect Network Access Attempt** detects when a device attempts to join the network or immediately after the attempt. This functionality should be achieved through integration with existing CDM HWAM functionality or through enhancement of the existing HWAM functionality.
3. **Authenticate Devices**[28] authenticates the device based on agency policy. This functionality should have some integration with HWAM for hardware inventory lists. Authentication is considered broadly here and may include combinations of device or network attributes derived from Agency policy that offer some assurance network access privileges should be granted to that device.
4. **Check Device Cybersecurity Posture** checks device compliance with agency hardware and software configuration and patching policies either (1) pre-connect, through a continuous security posture check for previously approved assets, and execution of automated or semi-automated orchestration of remediation of failed compliance checks prior to continued network access, or (2) after a post-connect brief exposure to the device.
5. **Enforce Access Control** is the CDM NAC PEP. It permits access to a network only if a device is compliant with agency policies, for example, inventory status, hardware, software, configuration, and patching. If the device is not compliant, NAC will block or quarantine the device, per agency policy. The policy could be as simple as permitting or blocking network access or could be more complex, for example, placing the device into quarantine.
    - Blocking may involve closing network ports on endpoint switches to which unauthorized devices are attempting to connect or dynamically created port-based access control lists on endpoint switches.
    - Quarantine may be used to allow the device to become policy compliant. Other security services may be notified when a device is put into quarantine.
6. **Force Device Compliance** restricts access to portions of the network and forces patching or upgrading of a device that NAC has placed in quarantine due to failure to comply with agency policies.
7. **Log and Alert on NAC Events** logs NAC events, for example, devices allowed access to the network, devices blocked, and the reason for the event (policy violated), devices quarantined and the reasons, etc. and provides alerts to agency personnel and tools, per agency policy and Agency deployed log aggregation or SIEM.

[28] See CDM AV-2: "Device Type."

8. **Report on Policy Compliance** provides reports of interest, based on NAC logs, to assess events.

Figure 5 is a block diagram showing the relationship among the NAC functions.

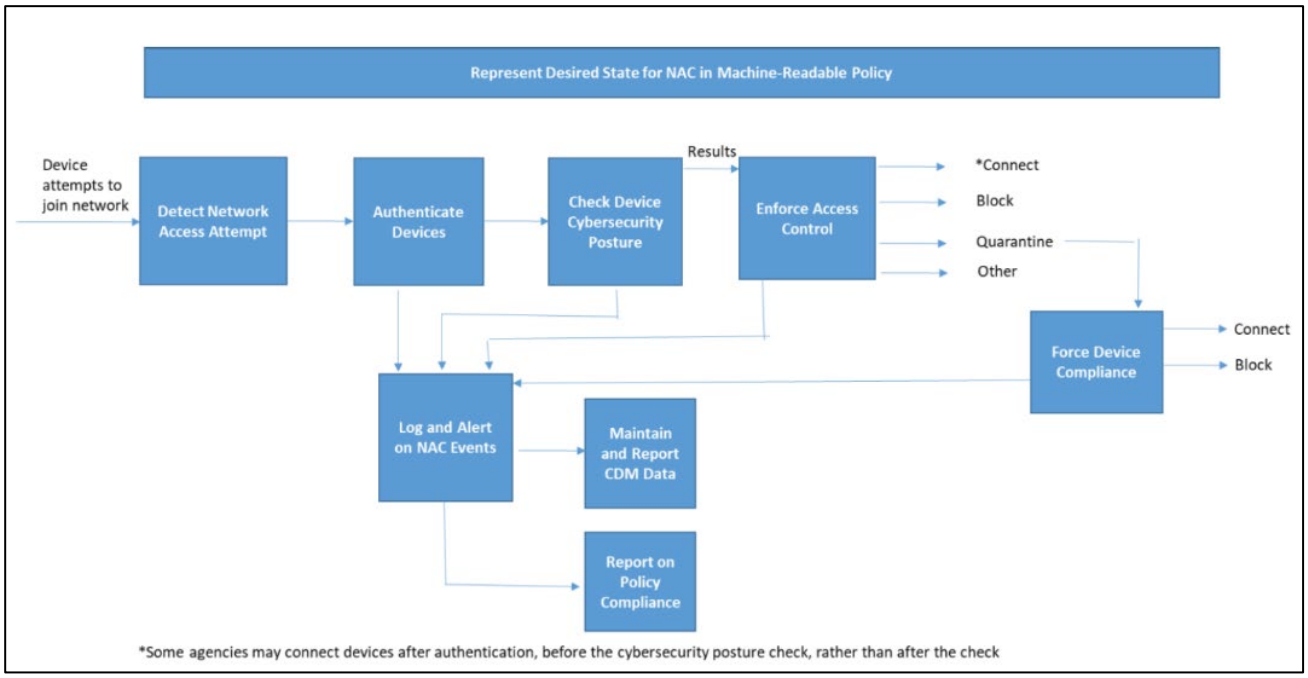

Figure 5. Workflow of Key NAC Functions

2.4.1.2.1 NAC Tool Functionalities

The following is a non-exclusive list of general tool functionalities that support the NAC functional requirements:

Tool Category Name	Summary of Functionality
Network Access Control technologies (implementing network control and/or agents)	Implement policies for controlling devices and user access to networks.
Identity and access management tools that integrate/implement with a control plane (to restrict or remove devices from the network)	Identifies and confirms users, applications, and devices. These will grant appropriate authorities and permissions. They can also establish and enforce policies and procedures that apply to user groups to include roles and responsibilities.
Passive and active asset management detection and scanning tools, including unified/ enterprise endpoint management tools (e.g., HWAM capability)	Identifies devices on the network.
Network segmentation tools/capabilities	Divides a network into multiple segments or subnets.

The following is a non-exclusive list of tools that NAC may integrate with:

Tool Category Name	Summary of Functionality
SIEM	Logging of CSM administrator actions and CSM management.
Firewalls	Monitors and controls incoming and outgoing network traffic.
Certificate generation tools (e.g., X.509 certificates, Public Key Infrastructure (PKI))	Generates certificates.
Key Management Orchestration	Orchestrated certificate and encryption key management.

2.4.1.2.2 NAC Functional Requirements

This section provides functional requirements for the NAC capability. The "shall" statements included in this set of requirements in Table 16 often require agency policy inputs to accurately develop machine-readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency. Note some of the NAC requirements were traceable to other parts of CDM and are listed for completeness.

Table 16. NAC Functional Requirements

Req. UID	Requirement Text
Represent Desired State for NAC in Machine Readable Policy	
NAC-1-1	The NAC capability shall implement NAC policies in machine readable format, as derived from agency policy.
	Guidance: Agency-derived machine-readable policies that are expected to be implemented by the NAC capability include any agency-defined policy that stipulates device-relevant cybersecurity posture requirements (e.g., patching baselines, virus scanner updates) that will be assessed as well as those derived rules for actions to be taken for non-complying devices (block, quarantine, etc.).
Detect Network Access Attempt	
NAC-2-1	The NAC capability shall detect between 95% (T) and 99% (O) of the devices attempting to gain entry to the network.
	Guidance: This may be detected through the presence of a new IP or MAC address on the network, or a new ESN/MEID, which could represent a new device trying to take over an existing connection. Traced performance to ORD KPP 2.b PROTECT - access control.
Authenticate Devices	
NAC-3-1	The NAC capability shall evaluate the network access privilege of each device with a false positive rate of no greater than 0.1% of total access connection attempts over a 30-day period, based on agency policy
	Guidance: Validation of network access privilege is expected to be primarily based on automated authentication rules, which may come from certificates, ACL, or other techniques and should conform to NIST 800-53 rev4 security controls such as SC-12. However, based on Agency policy and specific technologies such validation may also involve an indirect assessment of device attributes to validate network access privilege (e.g., patching status, configuration settings, etc.). *A false positive for this capability is defined as a scenario where the NAC capability evaluates a device and determines it is non-compliant to the Agency's policy when the device is actually compliant with the agency's policy.*
NAC-3-2	The NAC capability shall evaluate the network access privilege of each device with a false negative rate of no greater than 0.1% of total access connection attempts over a 30-day period, based on agency policy.
	Guidance: Validation of network access privilege is expected to be primarily based on automated authentication rules (i.e., NAC tool successfully authenticates to devices), which may come from certificates, ACL, or other techniques and should conform to NIST 800-53 rev4 security controls such as SC-12. However, based on Agency policy and specific technologies such validation may also involve an indirect assessment of device attributes to validate network access privilege (e.g., patching status, configuration settings, etc.). *A false negative for this capability is defined as a scenario where the NAC capability evaluates a device and determines it is compliant to the Agency's policy when the device is actually non-compliant with the agency's policy.*
Check Device Cybersecurity Posture	
NAC-4-1	The NAC capability shall check the cybersecurity posture of each device through compliance checks against an agency defined desired state, either before or after connection to the network, based on agency policy.

Req. UID	Requirement Text
	Guidance: "Cybersecurity posture" is a generic term to include agency-defined measurable configuration items on a device that can be associated with a potential reportable CPG (i.e., defect), which may be incorporated into a NAC capability decision to allow/prevent device access to the network
Enforce Access Control	
NAC-5-1	When configured by the administrator, the NAC capability shall block devices failing network access privilege validation from connecting to the network.
	Guidance: Some agencies may have a policy to block devices, others may quarantine.
NAC-5-2	When configured by the administrator, the NAC capability shall quarantine devices failing network access privilege validation from connecting to the network.
	Guidance: Some agencies may have a policy to block devices, others may quarantine.
NAC-5-3	The NAC capability shall connect devices complying with cybersecurity posture requirements to the network, per agency policy.
	Guidance: Some agencies may require a re-authentication. "Cybersecurity posture requirements" is a broad term to allow for agency defined rules such as patching currency, open vulnerabilities, configurations, etc.
NAC-5-4	The NAC capability shall block devices not complying with cybersecurity posture requirements from the network, based on agency policy.
	Guidance: Some agencies may have a policy to block devices, others may quarantine. Cybersecurity posture requirements" is a broad term to allow for agency defined rules such as patching currency, open vulnerabilities, configurations, etc.
NAC-5-5	The NAC capability shall quarantine devices not complying with cybersecurity posture requirements to the network, per agency policy.
	Guidance: Some agencies may have a policy to block devices, others may quarantine. Cybersecurity posture requirements" is a broad term to allow for agency defined rules such as patching currency, open vulnerabilities, configurations, etc.
Force Device Compliance	
NAC-6-1	The NAC capability shall force updates to quarantined devices to bring the devices into compliance with cybersecurity posture requirements, based on agency policy.
	Guidance: Some agencies may have a policy to force compliance, while others may not. "Forced compliance" could involve operating system upgrades, software installations, and configuration setting changes. Temporal service objectives (e.g., time to remediate cybersecurity posture gaps) related to this requirement will be based on or derived from available Agency policy.
NAC-6-2	The NAC capability shall connect devices forced into compliance to the network.
NAC-6-3	After a failed forced cybersecurity posture compliance attempt on a device, the NAC capability shall (1) Block the device (deny network access) or (2) Continue to attempt to force compliance for a configurable number of attempts while keeping the device in a quarantined state, per agency policy.
Log and Alert on NAC Events	
NAC-7-1	The NAC capability shall log data associated with authentication events, based on Agency policy.
	Guidance: This includes for example, authentication attempts and outcomes (devices blocked, quarantined).
NAC-7-2	The NAC capability shall log data associated with cybersecurity posture check events, based on Agency policy.
	Guidance: This includes for example, device identification, failed checks. See NIST ref AU-3.
NAC-7-3	The NAC capability shall log data associated with enforcing access control, based on Agency policy.
	Guidance: This includes for example, devices connected, devices blocked, devices put in quarantine, depending upon agency policy.
NAC-7-4	The NAC capability shall log data associated with forcing cybersecurity posture compliance, based on Agency policy.

Req. UID	Requirement Text
	Guidance: This includes for example, device identification, upgrades attempted, upgrades successful, upgrades failed, resulting cybersecurity posture compliance, depending upon agency policy. See NIST ref AU-1.
NAC-7-5	The NAC capability shall send alerts for logged events to configured distribution lists, based on Agency policy.
NAC-7-6	The NAC capability shall maintain logged data for the administrator configured time period, based on Agency policy.
Report on Policy Compliance	
NAC-8-1	The NAC capability shall generate reports, based on audit logs, upon administrator request.
	Guidance: These reports can be used in the manual audit process.
NAC-8-2	The NAC capability shall report a collection of NAC logs that includes the following information: • Device Metadata: Hostname, OS, IP address • NAC PEP outcome: Blocked, Allowed, or Quarantined • Timestamp of PEP outcome • Rationale of PEP outcome: agency policy breached/compliant to
	Guidance: This requirement is intended to be refined during solution engineering and integration to account for the specific data requirements outlined in supplemental, authoritative artifacts (e.g., CDM logical / physical data models, data requirement documents). Collected NAC logs are produced for CDM architecture consumption (e.g., CDM Federal/Agency Dashboards). Compliance state is intended to reflect whether a device passes the NAC PEP to the satisfaction of an agency's policy.

2.4.1.3 BOUND-E Requirements

The BOUND-E capability provides visibility into risks associated with the use of cryptographic mechanisms employed on an organization's network. Agencies use cryptography to protect credentials, data at rest, and data in motion.

BOUND-E provides the Agency indications of improper cryptographic behavior and/or of hardware/ software misconfiguration. If cryptography is used, cryptography must be properly implemented and configured to provide the desired level of protection. BOUND-E collects policies from hardware devices, software products, and cryptographic implementation configuration settings to ensure that the right (e.g., FIPS 140-2 validated) implementations are being used and configured properly.

The BOUND-E capability is further sub-divided into the following categories:

- Cryptography
  - Encryption Cryptography Technique
  - Hash Cryptography Technique
- Key Management/Certificate Authority (CA)
  - Key Management Design
  - Digital Signature Design
  - Certificate Authority Service

2.4.1.3.1 BOUND-E Operational Requirements

BOUND_OR-2-1: Shall afford protection to the confidentiality, integrity, and authenticity of data at rest, in transit, or in process via U.S. Government approved (e.g., FIPS 140-2 validated) cryptography.

BOUND_OR-2-2: Shall collect data associated with the boundary encryption policy and the encryption policy required for a network flow across a boundary to provide measurable data elements for the creation of automated security checks.

2.4.1.3.2 BOUND-E Functional Requirements

This capability requires CDM solutions to collect information when cryptography is used about attributes in the OU and FISMA containers, the MDR, the MUR, and the MSR. This capability is related to CRED if credentials

employ cryptography. This capability is also related to HWAM, SWAM, and CSM if system components employ cryptography. This capability is related to DATA_PROT, DATA_DLP, and DATA_IRM, which use cryptography to provide data protection.

BOUND_FR-2-1: If applicable, shall collect and report information related to:

a. The use of U.S. Government approved cryptographic algorithms as described in:
   i. Cryptographic Algorithm Validation Program (CAVP) https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program
   ii. National Security Agency's (NSA's) Suite B Cryptographic Program https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm.
b. The use of one-way cryptographic hash techniques to ensure the integrity of data, that is, to detect the alteration of the data at rest or in transit. The hash technique maps an input field of arbitrary size to a unique output field of a fixed size. The hash value of a given data can be used to determine if the original data was modified. Hash can be applied to either plain text data or cipher text data. The hash technique ensures the integrity of data at rest and in transit, and under certain designs can be used to support data confidentiality (e.g., password hash).
c. An approved key management process for generating, distributing, using, and destroying cryptographic key material. Keys are used to support confidentiality, integrity, authenticity, and secure communication between multiple users. The application of keys includes digital certificates, protection against the disclosure of information, identification of when data is altered, and verification of the authenticity of the data source.
d. Digital certification to provide proof of identity and authenticity. A digital certificate associates a public key with an owner. It provides two benefits: proof of origin (i.e., authenticity) and that the information was not altered (i.e., integrity).
e. A Certificate Authority (CA) that acts as a trusted third party to facilitate a secure communication between users over a PKI framework. Practical use of public key cryptography requires that whenever a relying party receives a public key said to be associated with an entity, someone or some organization that the relying party trusts must have vouched for the fact that the key does indeed belong with that entity.
f. The use of cryptography in application-layer protocols to ensure secure communication specifications for email communication, World Wide Web access, Domain Name System (DNS) validation, and secure remote logins to computing systems and other applications.
g. The use of cryptography in transport protocols that are not application specific and do not have any in-depth knowledge of the application behavior. Rather, the transport protocol focuses on the end-to-end connection between the communicating system, such as secure socket connection and connectionless communication.
h. Boundary cryptographic policies to determine what traffic can be encrypted/decrypted/signed/
hashed, and what traffic is blocked across a boundary. A boundary policy is the set of cryptographic policies for a boundary, including metadata about that policy.

2.4.1.3.3 BOUND-E Tool Functionalities

The following is a non-exclusive list of tool functionalities that support BOUND-E capability:

- Email digital signing technique to identity of the sender of the email message
- Digital key management systems
- Network access authentication using digital certificates
- Certificate management (creation, issuing, and revocation) systems
- Email encryption to obfuscate the content of the email message (e.g., Secure/Multipurpose Internet Mail Extension [S/MIME] encryption)
- DNS records signed using Domain Name System Security Protocol
- Secure remote logins (e.g., Secure Shell)

- Transport encryption at the link-layer (e.g., Media Access Control Security [MACsec])
- Network-layer (e.g., Internet Protocol Security [IPSec]) or transport-layer (e.g., Transport Layer Security [TLS], Datagram Transport Layer Security [DTLS]) security protocol used to protect data in transport across the network.

2.4.2 Manage Events (MNGEVT) Requirements

MNGEVT and OMI capabilities integrate to provide complementary processes and procedures to strengthen Agency's security postures.

The MNGEVT capability provides the identification of security threat vectors, detection of security violation events, and classification of event impacts. Endpoint Detection and Response (EDR) provides monitoring and control of endpoint devices. MNGEVT uses an incident management system to report and share events with OMI.

The Phase 3 MNGEVT capability covers the following areas:

- Incident response
- Privacy
- Contingency planning
- Audit and accountability
- Ongoing assessment
- EDR

2.4.2.1 MNGEVT Operational Requirements

2.4.2.1.1 Incident Response

MNGEVT_OR-1-1: Shall have policies and procedures for the implementation of controls and processes to perform incident response.

MNGEVT_OR-1-2: Shall implement methods to perform incident response, which may include one or more of the following:

1. Tracking incident response processes and procedures managed and maintained by a configuration management repository system.
2. Monitoring incident response policies for an Agency network and infrastructure by the ongoing assessment of security policies.
3. Sharing and communicating incident response about cyber threat information to internal and external organizations.

2.4.2.1.2 Privacy

MNGEVT_OR-2-1: Shall conduct security checks to verify that a privacy policy exists.

MNGEVT_OR-2-2: Shall notify data owners of data privacy breaches in accordance with Agency policies, applicable statutes, and regulations.

2.4.2.1.3 Contingency Planning

MNGEVT_OR-3-1: Shall have a contingency plan to restore and reconstitute full information system functionalities and the capability to apply new or additional security safeguards to prevent future compromise.

MNGEVT_OR-3-2: Shall implement contingency capabilities/functions/methods that may include one or more of the following:

- Backup and restoration methods, frequency and storage of backups, types of data to be archived, and the ability to restore data from appropriate backup storage devices to satisfy the Agency recovery time and recovery point objectives for the system.

- Geographically dispersed storage facilities to ensure continuity in the event the primary site is no longer accessible.
- Encrypting backup data as part of data backup per Office of Management and Budget Memorandum M-11-11 and performing integrity checks of backup data.
- Prioritizing Agency systems from highest to lowest regarding recovery/reconstitution based on the Agency's Business Impact Analysis.

2.4.2.1.4 Audit Data Collection

MNGEVT_OR-4-1: Shall have policies and procedures for the implementation of controls and processes to perform audit data collection.

MNGEVT_OR-4-2: Shall implement methods to perform audit data collection that may include one or more of the following:

a. Including operating system (OS) syslog, application log messages, system utilities monitoring logs, security activities log, abnormal application behavior, and network security activity logs.
b. Generating the following audit data:
    i. Appropriate audit data that can be used to support security assessment and forensic analysis
    ii. Audit records that meet regulatory requirements
    iii. Audit records that include "Who (asset or entity)," "What (action)," "When," and "Where (target)" attributes of log messages
c. Providing integrity-protected and/or tamper-evident functionality to provide evidence when the audit log data is compromised in transit or at rest.
d. Providing audit and accountability data to report authorization and authentication activities related to PII and protected critical infrastructure information access and disclosure.

2.4.2.1.5 Ongoing Assessment

MNGEVT_OR-5-1: Shall provide ongoing assessment data consolidation and assessment frequencies to deliver an effective continuous collection, analysis, and impact assessment of security policies in order to maximize automation and reduce human interaction.

MNGEVT_OR-5-2: Shall complete the ongoing assessment activities so that mitigation responses and operational recovery can be completed to reduce threat propagation to other Agency information and information systems.

2.4.2.2 MNGEVT Functional Requirements

2.4.2.2.1 Incident Response Monitoring

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers, the MDR, the MUR, the MSR, and the MIR. This capability is related to BEHAVE when behavior events related to incidents recorded in the MIR influence attribute values in the MUR. This capability is related to the DATA_SPIL capability for incidents involving the loss/leakage/spillage of information.

MNGEVT_FR_1-1: Shall collect and report information related to the implementation of methods to perform incident response and that enforce incident response policies. Information collected and reported may include one or more of the following:

a. Events and incidents related to malicious and/or anomalous activities that could impact the security posture of an Agency's network and infrastructure assets using data from HWAM, SWAM, CSM, VUL, BOUND, and DATA capabilities.
b. Initial analysis to determine incident severity based on the types of events, threat source, threat signatures, and impacted systems.

c. Workflow activities to maintain records for each incident, status of the incident, ability to annotate incident reports, and ability to request additional information that may be helpful in evaluating the incident from external system.
d. Complex aggregation and correlation algorithms using large volumes of stored data in a timely manner to generate incident reports.
e. Automated response to critical events based on severity and urgency by using an escalation technique to report the event.
f. Incident information (including analysis and alerts) aligned to incident response.

2.4.2.2.2 Privacy Monitoring

For privacy, the MNGEVT incident response security is augmented by additional policy requirements related specifically to privacy information. MNGEVT privacy covers various processes and procedures, some of which are automated and some that must be manually performed. For privacy, the automated policies for an Agency network and infrastructure will be enforced by the ongoing assessment of privacy policies for defects, which will be used to enhance or add new NIST SP 800-53 privacy controls and countermeasures. This capability is related to DATA for privacy related information.

The CDM solutions privacy information to be collected and relationship with CDM objects is covered in CDM Phase 4.

MNGEVT_FR_2-1: Shall continuously monitor for events and incidents related to privacy.

2.4.2.2.3 Contingency Planning Monitoring

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers, the MDR, and the MIR (as related to the activation of contingency operations). This capability supports data backup/restoration operations.

MNGEVT_FR_3-1: Shall collect and report information related to the implementation of capabilities/functions/methods for contingencies and that enforce contingency policies. Information collected and reported may include one or more of the following:

a. Backup operations related to contingency planning.
b. Actions to respond and recover from events in accordance with the contingency plan.

2.4.2.2.4 Audit Data Collection

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers, the MDR, and the MIR (as related to the incident data). This capability is related to CSM to ensure that auditing configurations are properly implemented on system components. This capability is related to all other capabilities that are sources of audit data.

MNGEVT_FR-4-1: Shall collect and report information related to the implementation of methods to collect audit data and which enforce audit data collection policies. Information collected and reported may include one or more of the following:

a. Audit/logging information that supports review, analysis, and reporting.
b. Audit/logging information in standard formats (e.g., syslog or Common Event Format) so that evaluation and correlation can be performed across multiple log sources.
c. Audit/logging information retention in a searchable, retrievable format for the appropriate timeframes according to retention policies and to support additional retrospective analysis.
d. Analysis and alerts for security policies aligned to audit and accountability.
e. Integration of operational log-based and NetFlow sources.

2.4.2.2.5 Ongoing Assessment Monitoring

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers. Ongoing assessment will require information about the attributes associated with the MUR, MDR, and MSR.

This capability is related to all other CDM capabilities for automated measurement of attributes supporting ongoing authorization.

MNGEVT_FR-5-1: Shall monitor for changes to the data elements/attributes for all CDM capabilities and report changes to OMI capabilities in order to support ongoing authorization.

2.4.2.2.6 Endpoint Detection and Response

The EDR capability provides cybersecurity monitoring and control of endpoint devices.[29] EDR spans the full cybersecurity lifecycle, from the detection of events (observable occurrences in a network or system) and incidents (events that have been determined to have an impact on the organization, prompting the need for response and recovery) on endpoint devices (i.e., workstations, servers, laptops, thin clients, and virtual desktops) and users, to attack responses and incident follow-up and analysis. EDR will also enforce the Agency's EDR administrator access policy based on user attributes and provide for delegation of administrative tasks. EDR is a sub-capability under MNGEVT in the Network Security Management Capability Area and is associated with the DETECT, RESPOND, and RECOVER functions as described in the NIST CSF. The EDR capability is expected to conform[30] with MITRE's adversary tactics, techniques, and common knowledge model (MITRE ATT&CK® matrix for enterprise) when producing alerts, reports, and/or any feedback to the administrator pertaining to observables events or artifacts on agency networks that provide Indicators of Compromise (IoCs) or Indicators of Attack (IoAs).[31]

Some of the functionality needed by EDR may be provided by other CDM capabilities with which EDR will interface. The CDM HWAM and SWAM capabilities are complementary to the EDR capability to identify devices and installed software.[32] Additionally, EDR may provide information to the following technology platforms, if implemented at the agency:

- SIEM – The EDR capability may provide endpoint event information to the SIEM. Additionally, SIEM platforms may provide threat intelligence information to the EDR capability.
- Security Orchestration, Automation, and Response (SOAR) – EDR provides endpoint incident information to a SOAR platform. SOAR platforms may carry out responses based on the EDR incident information. SOAR platforms may also provide threat intelligence to the EDR capability. The EDR capability can be integrated into SOAR playbooks or workflows. SOAR platforms may respond to the information received in accordance with the designed playbook, which may also direct the EDR capability to perform responses.

The following are the functions of the EDR capability:

1. **Configure EDR Security Policy** enables authorized users to implement and update agency EDR policy, including, for example, enterprise-wide alert and detection rules, automatic endpoint response actions, and endpoint agent scanning details. Custom plug-ins and scripts may also be configured and deployed to specific endpoints or

[29] EDR is scoped to integrate security functionality onto a subset of agency identified devices, which must be of category: ENDPOINT. In the requirements these devices are referred to as "endpoint devices." Refer to the CDM integrated program data dictionary (AV-2) and/or the CDM Data Model Document for more information regarding device categories. Agencies may additionally prescribe device sub-types for applicability of this capability (e.g., servers, desktops, laptops, etc.)

[30] See https://attack.mitre.org/ for additional information. Conformance to the MITRE ATT&CK matrix for enterprise includes aligning (i.e., referencing), minimally, adversarial tactics and techniques (sub-techniques are desirable if possible).

[31] Per the CDM Data Dictionary: An IoC is a technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred. IoAs, as used herein, focus on adversary behaviors and/or combinations of behaviors.

[32] Note that technologies that fulfill EDR capability requirements may also additionally perform HWAM and SWAM functionality and satisfy those capability requirements.

groups of endpoints. The policy includes the desired state information to support the PDP and PEP.

2. **Collect and Manage Cybersecurity-Relevant Endpoint Events** collects, organizes, and records cybersecurity-relevant endpoint event information and data artifacts (see requirements for a list of information collected).
3. **Maintain Endpoint Visibility** provides alerts on events and incidents and an authorized user on-demand query and display of live information about each endpoint (see requirements for a list of information collected).
4. **Support Incident Analysis** correlates collected cybersecurity-relevant events, forensic artifacts that have been identified through real-time monitoring and analysis, and threat intelligence. EDR provides detailed historic visualizations to support analysts in identifying and managing cyber incidents. This function will also automatically identify incidents.
5. **Threat Hunting** enables authorized users to discover current IoCs and IoAs related to known or suspected threats and to detect and monitor potential adversary patterns of activity and behaviors. EDR can leverage the community-supported specifications that report threat indicators and integrate with vendor-supported threat intelligence services to provide automated information sharing for cybersecurity situational awareness. Some examples are Structured Threat Information eXpression (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™). Cyber Observable eXpression (CybOX™) has been incorporated into STIX 2.0.[33] US-CERT Malware analysis reports.
6. **Maintain and Report EDR Data** provides for authorized user generation of reports and provision of EDR data to the agency. The Federal Incident Notification Guidelines[34] and/or the Federal Incident Response Requirements (FIRR) provide guidance on the data content.
7. **Respond to Incidents** provides or facilitates (through another platform) automated responses based on EDR information. In some cases, EDR would provide information to an orchestration function (i.e., SOAR platform) external to EDR that would coordinate follow-on responses. EDR can perform a standard set of remediation actions (e.g., isolate the endpoint, kill processes, quarantine files, etc.). Integrating with a SOAR platform can provide for a more robust and timely set of remediation actions that account for legal, policy, and technical considerations.
8. **Maintain Access Control** will control, delegate, and enforce EDR administrator access policies based on the user's role and Agency policy.

A functional block diagram to show the interaction of EDR functions (highlighted in blue) within EDR, as well as externally to EDR (orange boxes) or CDM third-party/external tools or capabilities (green boxes), can assist the team in identifying linkages and data transfer for requirements purposes. Figure 6 is a block diagram showing the relationship among the NAC functions.

[33] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity
[34] https://us-cert.gov/incident-notification-guidelines

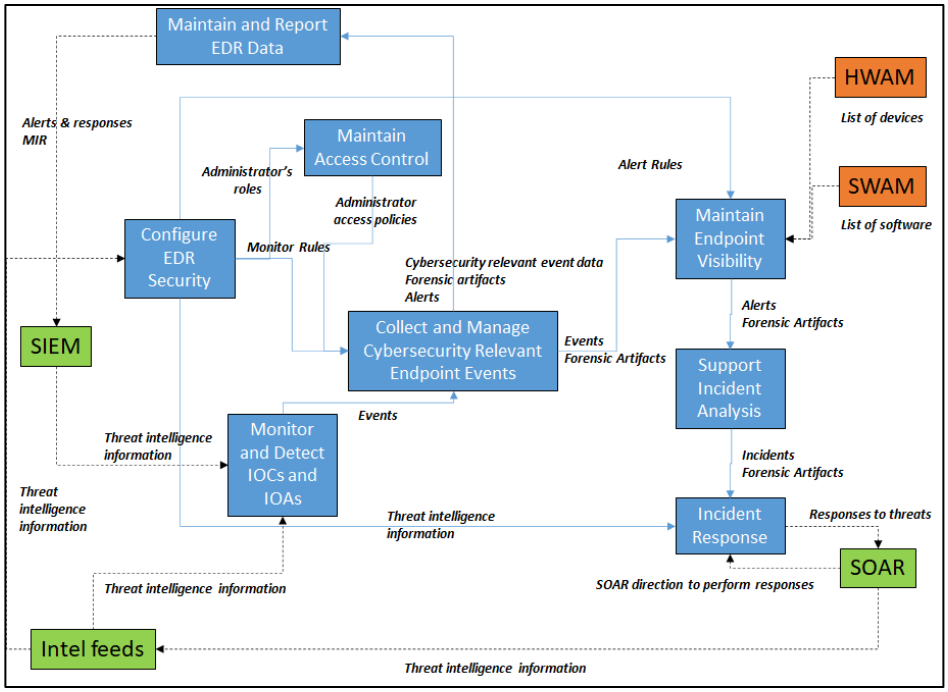

Figure 6. EDR Functional Block Diagram

The following is a non-exclusive list of general tool functionalities that support the NAC functional requirements:

Tool Category Name	Summary of Functionality
Endpoint Protection Platforms with EDR modules	Prevents file-based malware attacks, detects malicious activity, and provides investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.
Endpoint (Extended) Detection and Response tools	Takes a wider view than EDR, integrating security across endpoints, cloud computing, email, and other solutions.
Endpoint-based anomalous event detection tools (security alerts and notifications tools; suspicious activity detection of users, processes, data flows, behaviors, devices, and adversary tools)	Identifies data points, events, and/or observations that deviate from a dataset's normal behavior, which can indicate critical incidents or a change in behavior.
Search, event correlation, and post-incident forensic analysis tools	Uses log data to identify relationships and can relate various events to identifiable patterns.
Remote memory scanning and collection	Captures the memory of a suspected device to recover and analyze it.
At-scale raw forensic artifact collection	Collects and analyzes files and network activity to determine the scope, impact, and attribution of an incident.

2.4.2.2.6.1 EDR Functional Requirements

This section provides functional requirements for the EDR capability. The "shall" statements included in this set of requirements in Table 17 often require agency policy inputs to accurately develop machine-readable policies (i.e., tool configurations) that facilitate a true representation of an agency's desired state. CDM integrators are required to work with agency IT stakeholders to develop and incorporate those parameters in the final tool configurations to ensure successful operationalization of the CDM capability within an agency.

Table 17. EDR Functional Requirements

Req. UID	Requirement Text
Configure EDR Security Policy	
EDR-1-1	When configured by an administrator, the EDR capability shall implement EDR security policy for monitoring and alerting for an endpoint device(s).
	Guidance: This policy includes rules for monitoring and alerting on threats, adversary behavior, compliance, etc. Alert rules identify which events and incidents result in an alert notification, the content of the notification, and which users receive them. This provides the desired state for the Policy Decision Point (PDP) for generating alerts. See list of configurable cybersecurity relevant event data that may be monitored in EDR-2-1.
EDR-1-2	When configured by an administrator, the EDR capability shall implement out of the box monitoring and alert rules policies, aligned with the ATT&CK framework.
	Guidance: "Out-Of-The-Box (OOTB) functionality, policies, rules, etc. are offered through vendor tools, to the administrators, with minimal supplemental configuration. This includes turning the built-in monitoring and alert policies on/off and defining conditional execution. Tool vendors are aligning threat techniques with the ATT&CK framework, which may help to organize the monitoring and alert rules.
EDR-1-3	Upon input by the administrator, the EDR capability shall configure an agency's policy to implement a response action on an endpoint device.
	Guidance: This is the policy for the PEP for remediation (incident response based on configured endpoint response actions). Note that agency policy could be to implement no automatic response actions. See EDR-7-1 for information regarding response action functionality.
EDR-1-4	Upon input by the administrator, the EDR capability shall upload plug-ins to an endpoint device to add new functionality to the EDR capability.
	Guidance: "Plug-ins" are custom scripts and tools that potentially extend the capability of an existing agent, add a new agent, change the response path, etc. Agencies may require additional tools beyond the endpoint device for forensic / security purposes.
EDR-1-5	The EDR capability shall feature a console for administrators to centrally deploy and manage the endpoint agents across the agency network.
	Guidance: The intent of this requirement is to enable centralized administration of EDR agents, supporting viable scalability of the capability. See CMN-7-1 for additional information on capability scaling.

Req. UID	Requirement Text
Collect and Manage Cybersecurity Relevant Endpoint Events	
EDR-2-1	The EDR capability shall collect the following candidate cybersecurity relevant event data from endpoint devices: • Registry modifications, additions, deletions • Installed applications and status (running, suspended, and terminated) • Running processes and security components • Attached external devices • Services access (network ID requests/DHCP, proxy access, DNS queries, authentication server requests) • Network connection events • Account logins, remote and local • Permission changes • File Creation Time • File Modification Time • File attributes • Memory content and structures • Process information, including ancestry, privilege level, executing user, dll's and images loaded, other process and process memory accessed, process-to-process communications, process tampering • Remote thread creations (collected on the local system - could be created on the local system by a remote endpoint, or on the remote endpoint created by the local system) • Data transfer information (between applications on the device and between devices) • Configuration changes • OS-specific event logs • Audit log information based on anomalous activity • Scheduled Tasks
	Guidance: The specifics of the above data is intended to be refined through decomposition during solution engineering and to conclude at the System Design Review (SDR) milestone. *Examples on data types in this requirement:* *File Attributes: Static file attributes such as File size, digital signature presence/info, file path, file name.* *OS-specific event logs: Windows management instrumentation (WMI)* *Audit log information based on anomalous activity: unusual file access*
EDR-2-2	The EDR capability shall be interoperable with the following operating systems: • Client- and Server-based Windows OS [all Original Equipment Manufacturer (OEM)-supported variants] • MacOS (all OEM-supported variants) • Linux (all OEM-supported variants)
	Guidance: "OEM supported variants" mean operating systems that are current, actively supported by the software manufacturer (not end of life).

Req. UID	Requirement Text
EDR-2-3	The EDR capability shall provide the ability to collect the following candidate forensic artifacts: Program Execution -- • Browser history • Application execution (registry: e.g., Amcache, shellbags, recent files, DLLs) • Application pre-load (pre-fetch files) • Application terminations and cleanup (cache files, e.g., Shimcache) File Data – • Information on read, write, and deletion of data objects (files and heaps and stacks and AI linked lists) Network Information -- • DNS cache, • Remote Desktop Protocol sessions times, userIDs, and machines involved (source and destination), • Firewall rules, • Browser search terms, browser usage • Cookies, • External device/USB usage • History of connected networks Account Usage -- • Centralized) Network accounts (e.g., Active Directory), • Local accounts, • Authentication method employed (e.g., Multifactor, ID/PW)
	Guidance: The specifics of the above data is intended to be refined through decomposition during solution engineering and to conclude at the SDR milestone.
EDR-2-4	The EDR capability shall store collected forensic information for an agency defined time period.
	Guidance: The specifics of this information is intended to be refined through decomposition during solution engineering to conclude at the SDR milestone. *"Forensic artifacts" in the context of EDR include detailed investigative information beyond the traditional normalized CDM information covered in CMN-5-1 (e.g., Data in memory/Dumps, Device Event logs, information from examining raw disk/file systems) which may have high costs for long term retention.*
Maintain Endpoint Visibility	
EDR-3-1	The EDR capability shall automatically generate alerts based on tool vendor-provided or custom analytics which are mapped to the ATT&CK framework threat techniques when applicable.
	Guidance: EDR functionality includes vendor-provided analytics as well as the ability to create custom detections (to include adversarial technique signatures or identification of anomalies) that will automatically result in the generation of alerts, many of these may be based on the ATT&CK framework. If the ATT&CK framework does not cover the scope of the alert, then conformance to that framework is not applicable. This is part of the PDP. The policy of these alerts is based on EDR-1-2.
EDR-3-2	When configured by the administrator, the EDR capability shall generate alerts based on agency-defined alert rules.
	Guidance: Alerts can be associated with events, incidents, or other observables as derived by agency policy. These are additional configurations to enhance or tailor the PDP functionality that is pre-defined by the tool. The specifics of these alerts are intended to be refined through decomposition during solution engineering and integration to conclude at the System Design Review milestone.

Req. UID	Requirement Text
EDR-3-3	The EDR capability shall record the following EDR information for each alert: • Alert Unique ID • Date Time stamp • Detection Indicator (What triggered the alert detection (rule, heuristic etc.)) • Device and/or application ID (as applicable for the event) and owner UID (Where it happened) • Process and/or User ID (as applicable for the event) (Who/what caused the detection to happen)
EDR-3-4	The EDR capability shall display EDR information on the console, based upon one or more of the following administrator-selectable criteria: • Type(s) of information requested: • Alerts, Events, Forensic artifacts, IoCs/IoAs • Start and stop date and time of report window • Device types • Device Specific identifier • Endpoint Device Operating System • Endpoint processes and installed software • Login account information
	Guidance: See requirement EDR-3-3 for details regarding "EDR information". The intent of this requirement is to enable users to search for EDR information using configurable criteria. A device specific identifier may be an IP, MAC, hostname, and/or tool specific UID. This information can be exported if desired, per EDR-4-6. Active directory information (or an equivalent capability) may be used to collect information on user roles and capabilities to assist cyber incident investigations. Login account information may include items such as: user type, credentials, access rights, memberships, group policies, or computers used.
EDR-3-5	Upon input by the administrator, the EDR capability shall display the list of endpoint devices that do not have the EDR agent installed within the agency network.
	Guidance: This identifies the potential attack surface that is not covered by EDR protection and can be investigated to further implement EDR. HWAM provides the list of devices. SWAM discovers software installed on devices.
EDR-3-6	Upon input by the administrator, the EDR capability shall identify an alert as a false-positive.
	Guidance: This will allow the identified false positives to be filtered if desired.
Support Incident Analysis	
EDR-4-1	Upon input by the administrator, the EDR capability shall identify correlated EDR information as an incident.
	Guidance: Intent is for the tool to provide the analyst information and visualizations, per EDR-3-1 through EDR-3-6, which can be used to make a decision that an event, or multiple events, should be identified (i.e., declared) as an incident. This requirement provides the interface for the analyst to identify event(s) as incidents in EDR. This allows the administrator to call some correlation of information an incident, even though it is not identified as an incident in existing policy. See EDR-3-3 for the definition of "EDR information".
EDR-4-2	The EDR capability shall automatically identify incidents through correlation of cybersecurity relevant event information, data artifacts, and external threat intelligence (IoCs, behavioral information, etc.).
	Guidance: This is the EDR automated identification of incidents. Cybersecurity relevant event information is provided in EDR-2-1 and data artifacts in EDR-2-3. Behavioral information includes Tactics, Techniques, and Procedures (TTP)s and is provided in threat intelligence.

Req. UID	Requirement Text
EDR-4-3	Upon input by the administrator, the EDR capability shall display correlated cybersecurity relevant event information, incidents, alerts, forensic artifacts, and external threat intelligence, based upon any of the following selectable criteria: • ATT&CK framework (TTP) selection • Start and stop date and time of the report window • Device type • Specific device ID(s) (e.g., agency-defined unique specific ID such as host name, MAC address, tool specific UID) • Endpoint Operating System (e.g., operating systems such as Windows, Mac, Unix, Linux, iOS, Android) • Active processes that are running or in memory • User type, access rights, memberships, group policies, and computers used
	Guidance: This is to support analysts in assessing and managing cyber incidents, by acquiring greater detail. Active processes may include ones that are currently running or are in memory to identify actions performed by the system. Active directory information (or an equivalent capability) may be used to collect information on user roles and capabilities to assist cyber incident investigations.
EDR-4-4	Upon input by the administrator, the EDR capability shall display, on a console, a visualization of correlated cybersecurity relevant event information, incidents, alerts, forensic artifacts, and external threat intelligence (IoCs, behavioral information, etc.) across the network.
	Guidance: Data collected by EDR can help to identify affected components of the agency network as a result of endpoint activity and can help analysts trace the spread of affected endpoints in order to determine next steps. This is enabled by EDR-2-4.
EDR-4-5	Upon input by the administrator, the EDR capability shall display, on a console, an attack timeline of correlated cybersecurity relevant event information, incidents, alerts, forensic artifacts, and/or external threat intelligence.
	Guidance: An "attack timeline" will allow an administrator to see event information, incidents, alerts, and threat intelligence (IoCs, behavioral information, etc.) as a function of time to show when each happened relative to the other (e.g., process lineage).
EDR-4-6	When configured to export to third-party tools, the EDR capability shall export cybersecurity relevant events, forensic data, and/or threat intelligence data, based on agency policy configured, in industry-standardized data formats, including JSON and CSV, at a minimum.
	Guidance: Forensics artifacts should be exportable at scale to enable use of additional forensics tools or to provide to a third party to examine forensics data.
EDR-4-7	The EDR capability shall filter or sort retrieved data based on administrator selected criteria.
	Guidance: The specifics of retrieved data are intended to be refined through decomposition during solution engineering and integration to conclude at the System Design Review milestone.
Threat Hunting	
EDR-5-1	The EDR capability shall automatically detect indicators of compromise in and across endpoint devices, based on threat intelligence.
	Guidance: This is a threat hunting function. Malicious activity could be active in multiple endpoints, some of which may transfer malicious data / commands across endpoints. This would assist threat hunters in comparing the activity to IoC.
EDR-5-2	The EDR capability shall automatically search to detect adversary behavioral indicators using criteria compatible with the data model supported by the EDR tool and expressed in a query language that can be executed by end point devices, as configured based on agency policy.
	Guidance: The intent is for automatic detection of adversary behavior using agency derived customizations, which may include endpoint characteristics (e.g., OS, process metadata, network metadata, executable file metadata, Active Directory information, etc.). Searches may also look for hypothesized behaviors and correlation of events to aid threat hunters in detecting potential threats. Searches may also help threat hunters to query agency endpoints, times, activities to detect threats.

Req. UID	Requirement Text
EDR-5-3	Upon administrator input, the EDR capability shall search to detect adversary behavioral indicators using criteria compatible with the data model supported by the EDR tool and expressed in a query language that can be executed by end point devices, as configured based on agency policy.
	Guidance: This is the administrator-initiated search for indicators, while EDR-5-3 is the automatic search, as configured. The intent is for automatic detection of adversary behavior using agency derived customizations, which may include endpoint characteristics (e.g., OS, process metadata, network metadata, executable file metadata, Active Directory information, etc.). Searches may also look for hypothesized behaviors and correlation of events to aid threat hunters in detecting potential threats. Searches may also help threat hunters to query agency endpoints, times, activities to detect threats. Examples of such searches can be found in the Mitre Cyber Analytics Repository (https://car.mitre.org)
EDR-5-4	The EDR capability shall provide for the ability to search for indicators using industry-standardized formats.
	Guidance: Some common standard formats (e.g., Yara) should be able to be used to search for files and behaviors on hosts.
Maintain and Report EDR Data	

EDR-6-1	Upon input by the administrator, the EDR capability shall generate a report based upon the following selectable criteria:
	• Type of information requested (e.g., alerts, cybersecurity relevant event information, forensic artifacts)
	• Filters:
	  • Start and stop time of report window,
	  • Device category,
	  • Device types,
	  • Specific device identifier,
	  • TTPs from the ATT&CK framework.

EDR-6-2	The EDR capability shall integrate with agency SIEM platforms to report EDR alerts and associated responses.
	Guidance: See EDR-3-3 for details on alert data content. The alert information is from the PDP, while the response information, if applicable and included, is from the PEP. EDR data will be available through the EDR user interface (see Maintain Endpoint Visibility requirements). Intent is to integrate with pre-existing agency SIEM tools.
EDR-6-3	Upon administrator configuration, the EDR capability shall export endpoint event data (defined in EDR-2-1) to an external storage system (such as a SAN or NAS, cloud storage such as AWS S3 or Azure blobs)
Respond to Incidents	
EDR-7-1	The EDR capability shall execute a response action automatically upon detection of an incident on an endpoint, based on configured agency policy on endpoint response actions.
	Guidance: This is the PEP. Note that in agency networks having a SOAR capability, this requirement could be carried out in that external system, per agency policy. A "response action" is a generic term for describing actions that can resolve the potential threat and is expected to be technology specific and derived from agency policy. Response actions can include isolation/containment of the endpoint/threat from the network, killing processes/behaviors (i.e., eradication), quarantine of files, recording/logging the TTPs, and/or recovery activity as determined by the agency. (See NIST SP 800-61r2).
EDR-7-2	The EDR capability shall integrate with existing tools that are identified by the Agency to be part of the Agency's incident response workflow.
	Guidance: EDR needs to integrate with the Agency's incident response (IR) workflows, which may include integrating with deployed technologies that are critical to the IR process such as SOAR tools, IR reporting platforms/ticketing systems, etc.
Maintain Access Control	
EDR-8-1	Upon input by the administrator, the EDR capability shall delegate administrative tasks based on roles in accordance with Agency policy.

Req. UID	Requirement Text
	Guidance: Agencies create specific roles based on job functions, organizational assignments (e.g., sub-agency devices, users, federation, etc.), environmental factors, and the authorizations (i.e., privileges) to perform operations on security critical assets associated with the Agency-defined roles. The agency defines a set of agency-enterprise level policies that dictate how privileges can be controlled and delegated such that each sub-component within the agency maintains autonomy and control over assets that are uniquely assigned to that sub-component within the enterprise.
EDR-8-2	Upon login to the administrator's console, the EDR capability shall enforce the Agency's access policy based upon the attributes of the user's role.
	Guidance: This is a PEP that enforces access to objects and system functions based on the attributes of the user's role. See EDR-1-5 for the console requirement. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles.

2.4.2.2.7 MNGEVT Tool Functionalities

The following is a non-exclusive list of tool functionalities that support MNGEVT capability:

- Event-driven polling reporting approach
- Event-driven interrupt reporting approach
- Log management system
- Near real-time analytic
- Initial incident report generation
- Confidentiality of sensitive information
- Data minimization and retention for sensitive information
- Backup and restore method
- Agency recovery time objective/recovery point objective
- Forensic tools (e.g., file/registry/email analysis, disk capture)
- Network packet capture
- Forensic analysis tools

2.4.3 Operate, Monitor, and Improve (OMI) Requirements

OMI and MNGEVT capabilities integrate to provide complementary processes and procedures to strengthen Agency's security postures.

OMI focuses on the in-depth security root cause analysis, prioritization of security mitigation response/recovery, notification, and post-incident activity. OMI uses an incident report to share mitigation information with MNGEVT.

Ongoing Authorization dynamically monitors the security risk level using the results of MNGEVT ongoing assessment to detect when changing threats, vulnerabilities, technologies, and mission/business processes may result in an unacceptable security risk level.

Ongoing Authorization uses data from:

- The System and Information Integrity controls to assess the implementation efficacy of the NIST SP 800-53 controls to protect the Agency information and information systems.
- The Risk Assessment controls to dynamically assess the risk posture of the Agency information systems and if required, provide policy changes to MNGEVT.
- The Security and Assessment controls to identify vulnerabilities that could enable an attacker(s) to conduct malicious activities within an Agency's system. Once a vulnerability is identified by MNGEVT solution capabilities and it is determined that remediation is required, a Plan of Action and Milestones (POAM) will be developed to mitigate the vulnerability.

The products to support OMI capability must be able to enforce and update policies for all CDM solutions. The OMI capability covers the following areas:

- Ongoing Authorization
- System and Information Integrity
- Risk Assessment
- Security Assessment and Authorization

2.4.3.1 OMI Operational Requirements

2.4.3.1.1 Ongoing Authorization

OMI_OR-1-1: Shall provide a practical approach to perform reasonable assessment frequencies that will provide, consistent with Agency policy and maturity, continuous collection, analysis, and risk assessment of security-related policies on information and information systems using automation to limit human interaction.

OMI_OR-1-2: Shall complete the Ongoing Authorization risk assessment activities so that mitigation responses can be completed to reduce the potential lateral movement of threat propagation to other Agency information and information systems.

OMI_OR-1-3: Shall be used to ingest and export security authorization package information that includes POAMs, security plans, and security assessment reports to and from the appropriate internal and external stakeholders.

2.4.3.1.2 System and Information Integrity

OMI_OR-2-1: Shall have policies and procedures for the implementation of controls and processes to maintain system and information integrity.

OMI_OR-2-2: Shall implement methods to maintain system and information integrity that may include one or more of the following:

a. Flaw remediation functionalities.
b. Recommended mitigating solutions appropriate to the required protection level for the system.
c. Detecting anomalous and suspicious network, system, application, and user behaviors (e.g., unauthorized access, modification or deletion of information, anomalous traffic/event patterns).

2.4.3.1.3 Risk Assessment

OMI_OR-3-1: Shall have policies and procedures for the implementation of controls and processes to perform risk assessments for information systems.

OMI_OR-3-2: Shall implement methods to perform risk assessments that may include one or more of the following:

a. Dynamically assess the risk posture of its information systems and ensure that appropriate stakeholders participate in monitoring, assessing, and responding to risks against its information systems.
b. Determine which security controls need to be augmented or modified to maintain an acceptable level of risk

2.4.3.1.4 Security Assessment and Authorization

OMI_OR-4-1: Shall have policies and procedures for the implementation of controls and processes to perform security assessment and authorization for information systems.

OMI_OR-4-2: Shall implement methods to perform security assessment and authorization that may include one or more of the following:

a. Sharing security assessment results with authorizing officials and/or designated representatives in support of security authorization decisions.
b. Developing POAMs based on identified weaknesses and/or deficiencies and updating POAMs based on findings from security controls assessments, security impact analyses, and continuous monitoring activities.

2.4.3.2 OMI Functional Requirements

2.4.3.2.1 Ongoing Authorization

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers. Ongoing authorization will require leveraging information about the attributes associated with the MUR, MDR, and MSR. This capability is related to DATA_SPIL for incidents involving sensitive (especially privacy) data.

OMI_FR-1-1: Shall monitor (and report) the overall risk score for information systems, taking into consideration the presence of mitigations and countermeasures (e.g., POAM, compensating controls/processes), comparing that score with objective and threshold risk scores to support Ongoing Authorization decisions.

2.4.3.2.2 System and Information Integrity

This capability requires CDM solutions to collect information about attributes in the MDR. This capability is related to HWAM, SWAM, CSM, BOUND-E, and DATA_PROT in that hardware inventory, software inventory, and configuration settings are components of system and information integrity that need to be maintained. Remediation actions will require CDM solutions to collect information about attributes in the MIR. This capability is related to the DATA_SPIL capability for incidents involving the loss/leakage/spillage of information. This capability is related to DATA_DLP when security orchestration is used for event/incident response. This capability is related to BOUND-E and DATA_PROT to maintain information integrity.

OMI_FR-2-1: Shall collect and report information related to the implementation of methods to maintain system and information integrity and enforce system and information integrity policies. Information collected and reported may include one or more of the following:

a. Security posture changes or changes that affect the efficacy of NIST SP 800-53 security controls and countermeasures to mitigate component weaknesses and vulnerabilities for system and information integrity.
b. Vulnerability and threat remediation through response and recovery actions using automation to limit human interaction.
c. Protections from malicious code, actions, and threats and mitigation implementation when threats or malicious activities have exploited vulnerable conditions using automation to limit human interaction.
d. Incident information (including analysis and alerts) aligned to system and information integrity and integrating security and operational functionalities to support event response, including flaw remediation and incident management.

2.4.3.2.3 Risk Assessment

This capability will require CDM solutions to collect information about attributes in the MDR, MUR, MSR, and MIR for use in risk scoring.

OMI_FR-3-1: Shall collect and report information related to the implementation of methods to perform risk assessments and that enforce risk assessment policies. Information collected and reported may include one or more of the following:

a. Continuously monitoring for incidents to support the categorization of systems, applications, and data sensitivity as well as the impact on mission essential/business functions within the Agency.
b. Integration with VUL and DBS to include the results of vulnerability scans in risk assessment decisions.

c. Incident information (including analysis and alerts) aligned to risk assessment.

2.4.3.2.4 Security Assessment and Authorization

This capability requires CDM solutions to collect information about attributes primarily in the OU and FISMA containers. System interconnections will require information about the attributes related to the CSM components associated with the MDR and MSR. Any information related to incidents requires CDM solutions to collect information about attributes in the MIR.

OMI_FR-4-1: Shall collect and report information related to the implementation of methods to perform security assessment and authorization and enforce security assessment and authorization policies. Information collected and reported may be related to one or more of the following activities:

a. Identifying internal and external system interconnections that match those requiring BOUND filtering policies.
b. Developing plans of action for mitigation and remediation of security policy defects that cause unacceptable levels of risk. This may include authorized workflows to identify and execute response and recovery actions.
c. Performing trend analysis of continuous monitoring data to identify systemic trends in risk posture changes.
d. Analyzing and alerting on security policies aligned to security assessment and authorization.

2.4.3.2.5 OMI Tool Functionalities

The following is a non-exclusive list of tool functionalities that support OMI capability:

- Anomalous behavior detection (e.g., NetFlow analysis)
- Patch (OS and application) management system for flaw mitigation
- Impact (including function, information, and mission/business) analysis tools
- Advanced analysis and visualization tools to identify response and recovery actions
- Mission essential/business function cyber dependency mapping (Business Impact Analysis)
- Threat intelligence feeds for Risk Assessment
- Security testing tools to support Risk Assessment

2.4.4 Design and Build in Security (DBS) Requirements

The DBS capability addresses software acquired or newly developed to ensure that security and privacy is built in during all stages of the System Development Lifecycle (SDLC). DBS and the Supply Chain Risk Management (SCRM) concepts are used to reduce the attack surface for network and infrastructure components in the Design, Development, and Deployment areas of the system component SDLC.

"DBS Design" means to design the system components that will be used for this system. "DBS Development" addresses the use of that development environment (i.e., it covers the system development). "DBS Deployment" covers how agencies verify that the installed and running system is as it was designed and developed (i.e., that nothing has been changed or omitted).

The DBS Design area focuses on identifying and establishing motivation and goals for information and information system security and privacy needs. This includes assessing the environment risk posture and the design to mitigate those risks. Assessing the risk posture in the DBS Design area requires defining the security Concept of Operations (CONOPS) related to the business or mission needs, risk analysis, and assessment in order to identify potential weaknesses and vulnerabilities, and mandated policies related to regulation, governance, and compliance. This will enable the security architect to initiate a design that can incorporate appropriate security safeguards.

The DBS Development area focuses on developing and testing the information system to ensure that information system security and privacy needs are implemented effectively. This includes implementing secure coding practices, ensuring safeguards for sensitive information, and identifying and addressing security

weaknesses and vulnerabilities. Secure coding practices include fail-safe coding, critical code review, and secure code re-use. Weaknesses and vulnerabilities in this area are identified using a variety of testing methods on both source and compiled code. The Development area of the SDLC incorporates configuration and version management to track and minimize the introduction of errors (weaknesses and vulnerabilities) into information systems. Weakness and vulnerability testing supports the ability to identify and remediate errors that are introduced during the development of information systems.

The DBS Deployment area focuses on verifying that information system security and privacy needs have been met, to include the provenance of system components, securely deploying the information system, and maintaining the security control updates of the information system during operation. Securely deploying the information system in this area requires that the system installation is performed in a secure manner and that the information system is hardened (using secure configuration baselines). Maintaining information security in this area requires continuously monitoring the security posture of the information system and applying patches to mitigate vulnerabilities. The Deployment area of the SDLC incorporates release management to ensure that only versions of information system components that have properly completed development are deployed. Secure configuration baselines are developed and maintained to support secure installation and operation.

The SCRM area focuses on acquisition activities to help ensure that security goals are established and monitored. Such activities include sourcing of software, software purchase, mitigation of counterfeits, reputation scoring, and chain of custody.

2.4.4.1 DBS Operational Requirements

2.4.4.1.1 DBS Design

DBS_OR-1-1: Should identify relevant regulations, governance processes, compliance policies, and security CONOPS that malicious actors could exercise to compromise the information and information system and perform risk assessment to evaluate impact to information and information systems.

DBS_OR-1-2: Should implement methods to minimize vulnerabilities or weakness during information system design activities, which may include one or more of the following:

a. Optimizing information system security using threat modeling to identify objectives and vulnerabilities and define countermeasures to prevent and mitigate the effects of threats to the system.
b. Using techniques to identify and eliminate available avenues of attack to information systems.
c. Implementing secure architecture and defense-in-depth design principles to ensure that security and software robustness are built in throughout the SDLC, preventing single points of failure in security mechanisms for the information system.

2.4.4.1.2 DBS Development

DBS_OR-2-1: Should implement secure coding practices (including fail-safe coding, critical code and data protection, and secure code re-use) during information system development, which may include one or more of the following:

a. Implementing robust configuration, change, and version management during information system development.
b. Implementing the appropriate spectrum of testing (e.g., blackbox, whitebox, penetration, misuse case, dynamic and static analysis) to identify weaknesses and vulnerabilities during information system development (including scripts, batch files, and "applications" that are unique to the Agency).

2.4.4.1.3 DBS Deployment

DBS_OR-3-1: Shall execute secure acquisition (e.g., verify procurement supply chain, chain of custody) and disposal of components and data as part of information system deployment, which may include one or more of the following:

a. Implementing robust release management (including patches and security patches) as part of information system deployment.
b. Implementing secure installation principles (including hardening of systems and applications) as part of information system deployment.
c. Implementing methods to instrument and monitor runtime execution and track problems as part of information system deployment.
d. Implementing digital signing of software and signature verification to ensure the authenticity (provenance and integrity) of software components.[35]

2.4.4.1.4 DBS SCRM

DBS_OR-4-1: Should follow SCRM policies and procedures for baselining, tracking, and auditing the provenance of information system components (to include mitigation of counterfeits, reputation scoring, and chain of custody) for the acquisition/development of the information system.

DBS_OR-4-2: SCRM should be an integral part of the overall risk management process and include risk assessment guidance and the use of security related controls to mitigate identified risk.

DBS_OR-4-3: SCRM should establish a process for identifying, preventing, assessing, reporting, and mitigating the risks associated with the global and distributed nature of CDM product and service supply chains. The range of countermeasures selected The CDM Solution shall include appropriate risk reduction strategies and the best way to implement them.

2.4.4.2 DBS Functional Requirements

2.4.4.2.1 DBS Design

This capability will require CDM solutions to collect information about attributes in the FISMA containers. This capability is related to VUL attributes related to the software components associated with the MDR and adds provenance of information system components to SWAM attributes. This capability is related to DATA_DISCOV to determine the classification of data to be processed by a system.

DBS_FR-1-1: Shall collect and report information related to the implementation of modeling threats to information systems, including identifying vulnerabilities and corresponding countermeasures. Information collected and reported may be related to one or more of the following activities:

a. Identifying the possible attack surface of information systems.
b. Managing system/software security design and development requirements.

2.4.4.2.2 DBS Development

This capability will require CDM solutions to collect information about attributes in the FISMA containers. This capability is related to VUL attributes related to the software components associated with the MDR and adds provenance of information system components to SWAM attributes. This capability is related to DATA_PROT when data masking/obfuscation is used to generate test data to support the development process. This capability is related to DATA_SPIL when the breach/spillage is related to weaknesses in development or supply chain.

[35] Implementing digital signing and signature verification of software will require that additional attributes related to the certificate information of the signer (using the appropriate attribute information from BOUND-E) be collected by CDM Phase 1 SWAM (in addition to other provenance and reputation attributes about the software).

DBS_FR-2-1: Shall collect and report information related to the implementation of methods for secure information system development and enforce secure information system development policies. Information collected and reported may be related to one or more of the following activities:

a. Configuration management, change control, and versioning for information system security artifact development.
b. Testing for weaknesses and vulnerabilities in information systems. These vulnerabilities should include those identified by the VUL capability.

2.4.4.2.3 DBS Deployment

This capability requires CDM solutions to collect information about attributes in the FISMA container and MDR. This capability is related to CSM where the initial configuration at deployment of the system and after system update become part of the baselines and benchmarks for CSM. This capability also is related to SWAM and CSM for releases and patches to update information about the SWAM and CSM attributes related to the software components associated with the MDR.

DBS_FR-3-1: Shall collect and report information related to the implementation of methods for secure information system deployment and enforce secure information system deployment policies. Information collected and reported may be related to one or more of the following activities:

a. Managing releases and patches for information systems.
b. Developing and maintaining secure configuration baselines for information systems and information system components.
c. Instrumenting and monitoring information systems at runtime.
d. Tracking problems associated with information systems at runtime.
e. Digitally signing software before deployment.[36]

2.4.4.2.4 DBS Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the above DBS functional requirements:

- Application analysis for Common Weakness Enumerations (CWEs)
- Vulnerability scanners for CVEs
- Requirements change management and traceability tools
- Version and change control system
- Blackbox/whitebox/penetration testing
- Static/dynamic code analysis
- Patch management tools
- Deployment and release management tools
- Attack surface mapping and analysis tools
- Hardening operating system tools
- Problem tracking tools
- Software signing tools

2.5 Data Protection Management (DPM) Capability Area

Data Protection Management (DPM) Capability Area focuses on "How is data protected?" and builds on the CDM capabilities provided by Asset Management, Identity and Access Management, and Network Security Management.

[36] Implementing digital signing of software will require that additional attributes related to the certificate information of the signer (using the appropriate attribute information from BOUND-E) be collected by CDM Phase 1 SWAM (in addition to other provenance and reputation attributes about the software).

DPM focuses on the protection of sensitive (especially privacy) data,[37] which is covered by the following five capabilities:

1. Data Discovery/Classification (DATA_DISCOV) (Section 2.5.2) describes techniques for the identification, discovery, and classification of data.
2. Data Protection (DATA_PROT) (Section 2.5.3) describes data protection techniques.
3. Data Loss Prevention (DATA_DLP) (Section 2.5.4) describes techniques to minimize the loss of data.
4. Data Breach/Spillage Mitigation (DATA_SPIL) (Section 2.5.5) describes techniques for response and recover activities due to data breach/spillage.
5. Information Rights Management (DATA_IRM) (Section 2.5.6) describes data protection functions specific to information rights management.

Sensitive (especially privacy) data requires security and privacy protections at rest, in use, and in transit, to ensure the confidentiality, integrity, and availability of data assets, and to ensure that sensitive information is subject to authorized access and use only.

DPM covers the establishment of policies and management of data protection processes for the following:

- Identify sensitive (especially privacy) data assets
- Know where the data asset resides and the associated data flows
- Classify the data assets based on severity and impact
- Identify authorized roles, users, uses, processing, disclosures, and retention of privacy data
- Establish access controls and protection safeguards, commensurate with data asset severity and impact
- Monitor the efficacy of the data asset controls and safeguards
- Collect and report on data asset compromise
- Timely response to notify stakeholders of data breach or spillage
- Effective recovery to support operational and mission success

The enhanced data protections discussed within this section use the National Archives and Records Administration's (NARA) Controlled Unclassified Information (CUI) registry[38] as the source definition for "sensitive unclassified information" (i.e., sensitive data). This includes sensitive information subject to privacy protections (i.e., privacy data).

2.5.1 Common Data Protection Requirements

Common Data Protection requirements describe data constructs applicable to the five subsequent data protection capabilities identified in Sections 2.5.2 through 2.5.6.

DATA_ALL_FR-1-1: Shall provide protection for sensitive (especially privacy) data storage locations for the following non-exclusive list:

- Multiple operating system platforms
- Servers
- Workstations
- Laptops
- Mobile devices
- Cloud computing environments

[37] Privacy data includes Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI), among others.
[38] See https://www.archives.gov/cui/registry/category-list.

DATA_ALL_FR-1-2: Shall provide data and privacy protection for sensitive (especially privacy) data for storage types for the following non-exclusive list:

- Removable devices
- Disk Drives
- Files/Folders
- Databases records and fields
- Data stores (e.g., Databases, SharePoint, Outlook)
- Application Data (e.g., source code, executables, libraries, scripts)
- Tools and utilities (e.g., spreadsheet, browsers, word processing, email, Adobe)

DATA_ALL_FR-1-3: Shall provide data protection for sensitive (especially privacy) data formats for the following non-exclusive list of data types:

- Structured data formats (e.g., database, spreadsheet, metadata)
- Unstructured data formats (e.g., image file, multimedia, plain text)

DATA_ALL_FR-1-4: Shall provide collection, analysis, and reporting functions related to the auditing of data constructs associated with the implementation and management of data protection policies.

2.5.2 Data Discovery/Classification (DATA_DISCOV) Requirements

DATA_DISCOV products provide consistent identification of "data assets" across the organization for processing, storing, and transmitting information at all sensitivity levels. These products include the following capabilities and functions:

- Automated Data Discovery, which is a function where the Data Protection system crawls targeted databases to discover categorized columns that contain data subject to privacy (e.g., user names, Social Security Numbers, addresses, etc.). The output is then returned to a repository for reporting or other data protection capabilities.
- Data Classification, which is the ability of a system to create multiple levels of classifications to be assigned to system data. Classifications are then assigned to functions in a system to track data use, monitor user access to data, or assign protection functions, such as data masking.
- Data Tagging, which supports data identification and applying the appropriate data protection mechanisms.

Data Discovery/Classification capabilities can also be leveraged to enhance protections afforded to sensitive information such as PII. By knowing where sensitive data, especially privacy data, is located:

- An Agency is better positioned to meet:
  - Inventory requirements;
  - Monitoring requirements;
  - Authorized access requirements; and
  - Retention and disposal requirements.
- Unnecessary and unauthorized replication of sensitive information can be eliminated (e.g., assist with meeting associated statute requirements).
- Synchronization mechanisms can assist in ensuring that sensitive information, regardless of its location, is accurate, timely, complete, and relevant (i.e., the information is being maintained).

Access control mechanisms will better ensure that sensitive information is accessible only to authorized devices and authorized users for authorized purposes.

2.5.2.1 DATA_DISCOV Operational Requirements

DATA_DISCOV_OR-1-1: Shall define the types and characteristics of sensitive (especially privacy) data that will be used to identify different types of data in software applications, utilities, and libraries regardless of platform, data format, or storage type.

DATA_DISCOV_OR-2-1: Shall define different levels of data classifications that will be used to scan, identify, and categorize sensitive (especially privacy) data.

DATA_DISCOV_OR-3-1: Shall define the data tagging, labels, and/or metadata that will be used to assign different granularities and logical groupings of data, data records, and data fields.

2.5.2.2 DATA_DISCOV Functional Requirements

The DATA_DISCOV capability is essential to DATA_PROT, DATA_DLP, and DATA_SPIL to determine what data should be protected, how the data should be protected, how to minimize the loss of such data, and required actions for mitigation of the loss of such data.

This capability is related to MNGEVT as a log generation and utilization capability.

DATA_DISCOV_FR-1-1: Shall scan each data storage device on the network on a scheduled, event-driven, and/or ad hoc basis as specified by authorized users for sensitive (especially privacy) data using various types of contextual, inference, signature, and pattern matching searches, and filter the results based on level of the classified data.

DATA_DISCOV_FR-1-2: Shall report audit trail information related to the execution of data discovery capability.

DATA_DISCOV_FR-2-1: Shall categorize data based on classification of data as outlined by NARA CUI categories, government privacy-related guidelines, and applicable regulations.[39]

DATA_DISCOV_FR-2-2: Shall report data classification policies associated with different levels of data categories based on data relevance and impact to an organization. This policy-to- data-category mapping will be used as input to a system to track, monitor, and assign protection functions.

DATA_DISCOV_FR-3-1: Shall tag data using defined tags based on the result of data classification activities.

DATA_DISCOV_FR-3-2: Should report on the data tagging construct showing the logical grouping of data and resources into named categories by commonalities and classifications, such as data of similar types, data with the same access control classes or categories, data which is privacy data, and data associated with resources that perform specific operations.

2.5.2.3 DATA_DISCOV Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the above DATA_DISCOV functional requirements:

- Visualization of classification results
- Classify data based on classifier type associated with data classification
- Maintain data dictionary terms and definitions
- Notification and workflow approval routing capability
- Rule-based data classifier
- Flexible tag creation and assignment tool
- Classification and categorization of data and data types

[39] Applicable regulations include Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, and others.

2.5.3 Data Protection (DATA_PROT) Requirements

The DATA_PROT capability addresses primarily two methods to protect the data itself. The first capability is the application of cryptographic methods, while the second capability "hides" sensitive data fields values using data masking or obfuscation methods. These are in addition to the standard method of controlling access privileges for all sensitive information. Key attributes required for data protection include:

- **Data Policy Management** – Ability of a data protection system to create custom policies based on laws, regulations, and program-specific rules, understand the combinations of sensitive data elements in the organization systems by classification level (user determined) and breach cost, and score the cost by sensitivity level.
- **User access and logging/monitoring** – A system function that enables system administrators to restrict access and functions of a given user or user class. This functionality may also log user activity and provide notifications of policy or rule breaches or attempts by a given user.

Cryptographic security includes both encryption and masking/obfuscation, such as hashing, and is already incorporated into CDM under BOUND-E functional requirements. Encryption protects confidentiality by translating sensitive data into another form that can only be accessed with the proper decryption key. Encryption can be used to protect data at rest and in transit. Protection for data at rest includes:

- **Application encryption** – An application that leverages encryption to protect any data it processes by leveraging system functionality that implements system policies (enforced), or user discretion (ad hoc).
- **File encryption** – Individual files are encrypted either based on system policies (enforced), or at the user's discretion (ad hoc).
- **Storage container encryption** – A data partition, volume, or mountable volume file that is encrypted.
- **Full disk encryption** – A device, operating system, or third-party application that automatically encrypts all data stored on a device.

Data Masking/Obfuscation are methods whereby an application will be programmed to replace data fields that contain sensitive data with substitution data that is generated based on a set of rules. Users who are not authorized access to the sensitive data, either through the native application or via database query, will have substitution data returned to them.

Data Masking/Obfuscation is a function that uses a set of rules to replace sensitive data. Multiple methods are used in masking and obfuscation. Data shuffling, scrambling, and encryption are functions that can be used to mask sensitive data. There are two types of data masking: static and dynamic. In static data masking, the sensitive data is masked and stored so that the data at rest is protected. In dynamic data masking, the sensitive data is masked prior to transit, leaving the data at rest unaltered.

2.5.3.1 DATA_PROT Operational Requirements

DATA_PROT_OR-1-1: Shall create and manage organizational data protection policies (e.g., cryptography, data masking/obfuscation, and access controls) using one or more PDPs.

DATA_PROT_OR-1-2: Shall create and manage organizational privacy protection policies that ensure privacy data is accessed, used, processed, retained, and disclosed as authorized in the cognizant Notice and applicable regulations.

DATA_PROT_OR-2-1: Shall establish policies to analyze the behavior of users and endpoints related to data access and use for alignment with the data protection mechanism.

DATA_PROT_OR-3-1: Shall define policies to protect data at rest using the U.S. Government approved cryptographic methods meeting BOUND-E operational and functional requirements to address one or more of the following: certificate management, application encryption, file encryption, storage container encryption, full disk encryption, or cryptographic anchoring.

2.5.3.2 DATA_PROT Functional Requirements

The DATA_PROT capability requires CDM solutions to collect information about attributes primarily in the OU and FISMA containers, the MDR (e.g., data categorization, data protection policies), and the MSR (e.g., boundary/interconnection between systems and the associated boundary filtering policies for sensitive data).

This capability is related to DATA_IRM and DATA_DLP when cryptographic data protection methods are employed.

This capability is related to BOUND-E through the use of encryption for data protection. This capability may integrate with BOUND-F to enforce data protection for data in transit. This capability is related to MNGEVT as a log generation capability and as an analytic tool to detect data protection events.

This capability is also related to DBS to support generating test/development data using data masking/obfuscation. This capability is related to MNGEVT as a log generation capability and as an analytic tool to detect data protection events.

DATA_PROT_FR-1-1: Shall automate the collection of audit trail information related to the creation and management of information protection policies, the execution of cryptographic methods meeting the BOUND-E operational and functional requirements for data protection, the implementation and operation of data masking/obfuscation, and the execution of access controls enforcement of data protection policies.

DATA_PROT_FR-2-1: Should perform user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration, and insider access abuse (including excessive or unauthorized access to data, functions, and privilege abuse) and provide context for security investigations.

DATA_PROT_FR-3-1: Shall perform cryptographic data protection, meeting BOUND-E operational and functional requirements, to reduce the risk of attacks and possible impact to data and operational processes. Cryptographic data protection may include one or more of the following: application encryption, file encryption, storage container encryption, full disk encryption, or cryptographic anchoring.

DATA_PROT_FR-4-1: Shall perform data masking/obfuscation to reduce the risk of attacks and possible impact to data and operational processes. Data masking/obfuscation may include one or more of the following: substitution, shuffling, numeric variance, redaction/suppression, tokenization, format preserving encryption, or de-identification/pseudonymity.

DATA_PROT_FR-5-1: Shall implement access controls to reduce the risk of unauthorized access to sensitive (especially privacy) data through the use of one of more of the following: discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), attribute-based access control (ABAC)[40], or adaptive access control/risk-based access control.

2.5.3.3 DATA_PROT Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the above Data Protection functional requirements:

- Cryptographic anchoring
- Discretionary access control
- Mandatory access control
- Role-based access control
- Attribute-based access control
- Adaptive access control/risk-based access control

[40] Also referred to as rule-based role-based access control (RB-RBAC). Next generation access control (NGAC) is also associated with ABAC. NGAC is a framework for implementing ABAC in an interoperable manner between systems. Another framework is eXtensible Access Control Markup Language (XACML).

- Application encryption
- File encryption
- Full disk encryption
- Storage container encryption
- Static data masking
- Extraction-transformation-load (ETL) data masking
- Dynamic data masking
- Substitution
- Shuffling
- Tokenization
- Numeric variance
- Redaction/suppression
- Format-preserving encryption

2.5.4 Data Loss Prevention (DATA_DLP) Requirements

DATA_DLP products provide consistent protection to block exfiltration of sensitive (especially privacy) data outside the organization inappropriately (i.e., outside a documented routine use), and use capabilities and functions that include the following:

- **Multi-platform capability/multi-database capability** – The ability of a system to be run on multiple operating systems or hardware platforms. The ability of a data privacy system to query multiple types of databases and report on them using a unified reporting system.
- Interpretation of system-readable policies and formalized connection agreements that instantiates security and privacy rules such as decisions related to authorized access to privacy data based on application, roles, and data type as specified in the cognizant Privacy Notices and applicable laws and regulations. The system supports responses including enabling, prohibiting, or quarantining access, as well as other types of enforcement actions.
- **Role/attribute-based data protection** – A data protection system function that allows a system administrator to assign data protection schemes (encryption, application and system access controls, hashing, substitution) to data elements in another system, and associate those schemes to defined roles. Users are then assigned to the roles.
- **Exfiltration alerts and prevention** – DLP tool functionality that monitors data movement through systems by user or system and is capable of restricting or limiting data movement based on rule sets or behavioral patterns including quarantining a system or user activity for further administrative review. The system reports or alerts any deviation from set boundaries or thresholds of data use.
- **Protection orchestration** – The ability of a data protection system to operate within a suite of tools, or integrate within a Security Information and Event Management (SIEM) infrastructure, to control and monitor data protection functions across systems, including encryption/decryption, data masking, exfiltration prevention, auditing and reporting, use authorization, etc.

DLP capabilities can also be leveraged to enhance protections afforded to sensitive information, such as PII, by:

- Enhanced monitoring and recognition of sensitive information traversing interconnections to ensure:
  - The exchange is restricted to authorized information;
  - The exchange is restricted to authorized purposes;
  - The exchange is restricted to authorized entities/users.
- Restricting the ability to create archival copies (e.g., backups) on unauthorized devices and media.

2.5.4.1 DATA_DLP Operational Requirements

DATA_DLP_OR-1-1: Shall create and manage DLP policies using one or more PDPs.

DATA_DLP_OR-1-2: Shall support DLP methods to protect data on endpoints (i.e., data at rest, data in use) and on the network (data in motion), utilizing one or more of the following:

a. Content monitoring and inspection
b. Contextual monitoring and analysis
c. Metadata/tagging monitoring and inspection

DATA_DLP_OR-1-3: Shall support regulation mandates on sharing of privacy data to include an Agency's Privacy Notice(s), an Agency's policy, and interconnection agreements on authorized endpoints and data paths.

DATA_DLP_OR-2-1: Shall support orchestration of data protection functions across platforms and between CDM data protection capabilities.

2.5.4.2 DATA_DLP Functional Requirements

The DATA_DLP capability is related to DATA_PROT when cryptographic data protection methods are employed and to DATA_PROT when data masking/obfuscation methods are employed as part of DLP protections. This capability is related to DATA_PROT through the use of fine-grained access control for data protection. This capability is related to DATA_IRM when information rights management policies trigger DLP prevention measures for data in transit.

This capability is related to PRIV, to support logical access control decisions for access to sensitive data. This capability is related to BOUND-E through the use of encryption for data protection. This capability may integrate with BOUND-F to enforce data protection for data in transit. This capability is related to MNGEVT as a log generation capability. This capability is related to OMI when security orchestration is used to respond to the data protection events/incidents.

DATA_DLP_FR-1-1: Shall provide audit trail information related to execution of DLP methods and the movement of data. The information will support the continuous monitoring and update of access DLP policies and administration activities to ensure enforcement of data protection policies.

DATA_DLP_FR-1-2: Shall perform DLP using one or more of the following DLP methods:

a. Encryption
b. Quarantine
c. Block
d. Notification
e. Allow with user justification

DATA_DLP_FR-1-3: Shall perform one or more DLP methods to reduce risk and potential impacts to data and operational processes. DLP methods may be implemented in one or more of the following:

a. Endpoint DLP monitoring, alerting on, and preventing used or manipulation of sensitive data by end-user activity (e.g., copy, paste, save, open, print operations, and screen captures) to detect or prevent data exfiltration.
b. Network DLP monitoring, alerting on, and preventing the movement of data over the network using various network protocols (e.g., email, web, file transfer, instant messaging) to detect or prevent data exfiltration.
c. User and/or system DLP monitoring to alert and prevent unauthorized use, storage, and transmission of privacy data by a user and/or system that has other legitimate access to the privacy data.

DATA_DLP_FR-1-4: Shall integrate DLP with other data use and protection capabilities to protect data and detect potential compromise. Other data protection capabilities may include one or more of the following:

a. Identity/attribute stores to provide federated identification, authentication, and attribute assertions
b. IRM solutions to protect information leaving an Agency, which may include the use of encryption or masking/obfuscation
c. Data repositories
d. Office automation applications
e. Cloud applications
f. Log/event analysis systems (e.g., SIEM, User and Entity Behavior Analytics [UEBA])
g. Enterprise Data Discovery solutions

DATA_DLP_FR-2-1: Shall perform orchestration of data protection functions across platforms and capabilities, such as encryption/decryption, data masking, exfiltration prevention, auditing and reporting, and access control.

2.5.4.3 DATA_DLP Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the above Data Loss Prevention functional requirements:

- DLP regulatory rules/policy interpretation and translation
- DLP endpoint functionalities
- DLP network inspection functions
- DLP alerts and notifications
- DLP incident report generation
- DLP blocking/quarantining function
- Security orchestration control and management of data protection capabilities

2.5.5 Data Breach/Spillage Mitigation (DATA_SPIL) Requirements

DATA_SPIL mitigation refers to policies, processes, and procedures that an organization develops in response to an unauthorized loss of organization data. Depending on the type of sensitive data, these policies and procedures may be unique. For example, there are severe reporting requirements for breaches and spills involving PII.

Systems and external service providers can assist organizations in legal/regulatory, media, and recovery/remuneration processes to the public or other bodies. Internal systems that organizations may implement can, in some instances, integrate with SIEM products to aid in data leakage/theft discovery, determining the responsible parties for loss and recovery, and what role each must take based on the data loss, management of the internal and external escalation processes, and the development and maintenance of workflows and response plans. Response to a loss of sensitive or privacy data must adhere to applicable statutes, regulations, and policies.

Data breach and spillage mitigation capabilities can also be leveraged to enhance protections afforded to sensitive information, such as PII, by:

- Assisting in achieving compliance with reporting requirements associated with the allowed uses of the sensitive information;
- Integrating management of reporting of incidents and breaches within incident response;
- Providing enhanced automation for incident and breach response processes;
- Improving monitoring, detection, and reporting of anomalous behavior involving sensitive information such as privacy data;
- Assisting in the response to anomalous behavior involving sensitive information such as privacy data

2.5.5.1 DATA_SPIL Operational Requirements

DATA_SPIL_OR-1-1: Shall create and manage policies and procedures that address systems and/or components associated with a data breach/spillage involving sensitive data or impacting privacy. Mitigation operations may include one or more of the following:

a. Supporting consistent, repeatable mitigation and recovery workflows and processes that:
   i. Identify logical or physical compromise of information, system(s), and/or component(s)
   ii. Identify other information sources, systems, and/or components that may have also been compromised
   iii. Isolate the compromised information, system(s), and/or component(s)
   iv. Restore/recover operations through mitigation and/or remediation
   v. Provide notification to data owners about the type of data spillage and impact
   vi. Support decision trees that drive the breach response
b. Establishing a shared mitigation notification between internal and external sources
c. Facilitating incorporation of breach changes driven by authoritative sources such as statute (law), regulation, and policy

DATA_SPIL_OR-1-2: Shall support the review of security/privacy reports and audit logs across all users and operational processes for evidence of activity that is indicative of a data breach/spillage incident involving, or impacting, sensitive data or privacy. Activities and sources may include one or more of the following:

a. Policy violations involving structured and unstructured sensitive data
b. Unauthorized or unexpected changes in behavior from users or processes with access to sensitive data
c. Audit/log data analysis systems (e.g., SIEM, UEBA)
d. Access management (e.g., authentication, authorization) and monitoring systems
e. Security devices (e.g., firewall, application firewall, malware detection)
f. Applications (e.g., services and web applications)
g. Infrastructure devices (e.g., network, communication devices)
h. Removable media/storage monitoring systems.

DATA_SPIL_OR-1-3: Shall support the review of existing security/privacy controls and countermeasures for determining when additional mitigation solutions are needed to reduce, if not eliminate, risks of data compromise or loss that can result from software and device weaknesses and vulnerabilities. Security/privacy controls and countermeasures may include one or more of the following systems that are:

a. Reducing risks from spam, viruses, and other malware
b. Identifying and destroying old or unused data
c. Identifying inadequate folder, file, and database protections
d. Identifying leaks
e. Reducing risks from the use of removable media (e.g., CD or DVD).

DATA_SPIL_OR-1-4: Shall support the creation and management of organizational response and recovery plans for the restoration of normal operations following a data breach/spillage incident that cover:

a. Compliance with organizational policies and authoritative requirements (e.g., statutes, regulations) to include requirements associated with privacy
b. Definition and establishment of appropriate data communication channels based on data classification
c. Notification of designated internal and external users/organizations (to include breach reporting) that includes sharing information to facilitate enhanced cybersecurity situational awareness across the organizational enterprise

d. Identification of:
    i. Organizational stakeholders (e.g., response staff, legal counsel, organizational management)
    ii. Mandatory response and recovery training for staff involved in response and recovery
    iii. Organizational impact (including impacted individuals, impact to reputation) from a compromise
e. Repair of reputation as part of restoration process
f. Integration of lessons learned for improvement

2.5.5.2 DATA_SPIL Functional Requirements

The DATA_SPIL capability is related to the DATA_DISCOV, DATA_PROT, DATA_DLP, and DATA_IRM capabilities in that the DATA_SPIL capability is the last line of defense when those capabilities fail to protect sensitive (especially privacy) data.

This capability is related to CSM, VUL, PRIV, CRED, MNGEVT, OMI, and DBS capabilities to monitor, access, and respond to security/privacy compromises to sensitive data.

DATA_SPIL_FR-1-1: Shall collect, analyze, and report security/privacy activities related to the execution of sensitive (especially privacy) data breach/spillage mitigations including suspected breaches. For privacy breaches, the information collected shall be reported to the cognizant Agency as soon as possible, and without unreasonable delay. The cognizant Senior Agency Officials for Privacy (SAOPs) for the applicable Agency shall collaborate with CDM to orchestrate the response, including identifying information that needs to be collected. Information collected, analyzed, and reported may be related to one or more of the following:

a. Creation and prioritization of remediation actions
b. Dynamic impact assessment quantifying incident severity, data sensitivity, and notification requirements
c. Unauthorized access to, or the potential unauthorized access to, sensitive (especially privacy) data by users and processes (i.e., access violations)
d. Access to privacy data by authorized users for unauthorized purposes
e. Leakage of sensitive (especially privacy) data (e.g., complete or partial leak)
f. Automation of and collaboration in mitigation workflow processes

DATA_SPIL_FR-1-2: Shall automate the collection, analysis, and reporting of compliance information to facilitate improved efficiency in and effectiveness of processes supporting identification and deployment of new sensitive (especially privacy) data protection mitigations. Information collected, analyzed, and reported may be related to one or more of the following:

a. Identifying gaps in meeting evolving regulatory policies and changing threats
b. Aligning sensitive (especially privacy) data policies with risk mitigation controls and countermeasures
c. Assessing mitigation controls and countermeasures to ensure effectiveness

DATA_SPIL_FR-1-3: Shall collect security/privacy information used in analysis and making mitigation and remediation decisions in a manner that is compliant with the Federal Rules of Evidence.

2.5.5.3 DATA_SPIL Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the above Data Breach/Spillage functional requirements:

- Identify specific data security/privacy controls that caused the data breach/spillage.
- Assess the effectiveness of controls to determine the areas of non-compliance.
- Provide the data that enables the cognizant Agency to assess the severity impact from a data breach/spillage incident, and derive risk mitigation strategies for the potentially impacted individuals.

- Provide tools to look across log files for related events to synthesize potential comprehensive breach scenarios.
- Assess the impact to organization normal operations.
- Generate incident report for internal and external organization.
- Send incident report alerts and notification to internal and external organization.
- Quantify the loss of sensitive (especially privacy) data.
- Compute mean time to recovery from data breach/spillage.
- Identify new or enhance existing data security and privacy controls to prevent further data breach/spillage.

2.5.6 Information Rights Management (DATA_IRM) Requirements

DATA_IRM controls access to enterprise information (e.g., documents, files). IRM solutions provide fine-grained and identity-aware protections that are persistent. IRM solutions generally employ:

- **Cryptography** – Sensitive data is encrypted so the confidentiality is maintained independent of location while in transit or at rest.
- **Granular control** – Entities are granted rights for access to the data (e.g., view, review, edit, print, copy/paste, or screen capture).
- **Identification** – Entities are authenticated before access is granted using policies based on roles and/or group membership.

IRM provides document (usually at the file level) encryption of sensitive data. As such, IRM solutions provide a key management function to control encryption/decryption of sensitive data. IRM can also be leveraged to enhance protections afforded to sensitive information, such as PII, by:

- Providing management of sensitive information that has been shared beyond an Agency's borders to ensure:
  - Only authorized information is being shared;
  - Only authorized entities/users have access to the sensitive information.
- Restricting the ability to access, create, modify, delete, or duplicate sensitive information (to include disallowing copying to unauthorized devices and media).

Access control includes managing identities used by external entities.

The centralized access control model for IRM supports the ability to monitor the use of data even when outside the Agency. Monitoring includes who accessed the data and what actions were taken on the data.

Because of the global (that is, being scoped outside of the Agency controlled space) nature of IRM, it is provided as a service (usually cloud based) to which the Agency subscribes.

2.5.6.1 DATA_IRM Operational Requirements

DATA_IRM_OR-1-1: Shall allow the creation and management of information rights management policies using one or more PDPs. Examples of IRM policy support include:

a. Policy management and policy-driven capabilities to monitor versioning, track changes, and manage workflows and simulations
b. Mechanisms to enforce IRM policies on what data can be accessed, by whom, from which locations, and using which devices

DATA_IRM_OR-1-2: Shall support the integration of IRM with enterprise products/services to facilitate enhancement of data protection and detection functions. Examples of enterprise products/services that can benefit from integration of IRM include:

a. Data repositories (e.g., file shares)
b. Office automation applications (e.g., email, word processing)

c. Cloud applications (e.g., file storage, service provider)
d. Log/event analysis systems (e.g., SIEM, UEBA)
e. Enterprise DLP solutions
f. Enterprise Data Discovery solutions
g. IdAM, to include attributes (e.g., Active Directory)
h. Multimedia collaboration and information sharing platforms supporting internal and external users

2.5.6.2 DATA_IRM Functional Requirements

The DATA_IRM capability requires CDM solutions to collect information about attributes in the OU and FISMA containers, the MDR (e.g., data categorization, data protection policies), the MUR (e.g., role), and the MSR (e.g., boundary/interconnection between systems and the associated boundary filtering policies for sensitive data).

This capability incorporates DATA_PROT through the use of fine-grained access control for data protection and/or through the use of encryption for data protection. This capability is related to DATA_DLP when Information Rights Management policies trigger data loss prevention data protection functions. This capability may incorporate DATA_DISCOV through the use of tags to support the enforcement of IRM policies. IRM solutions are complete systems that do not rely on related data protection capabilities as external items to provide IRM. IRM solutions generally integrate with related data protection capabilities to enhance overall data protection.

This capability is related to PRIV, TRUST, CRED, and BEHAVE attributes to support logical access control decisions for access to sensitive data. This capability also is related to BOUND-E through the use of encryption for data protection and with BOUND-F to enforce data protection for data in transit. This capability is related to MNGEVT and OMI as a log generation and analysis capability.

DATA_IRM_FR-1-1: Shall perform IRM functions to protect data and detect potential compromise. IRM functions include:

a. IRM protection/detection functions for one or more of the storage constructs
b. FIPS 140-2 compliant and NIST validated cryptographic module to encrypt sensitive data
c. Dynamic policies (i.e., fine-grained policy changes vice simple access revocation) including attribute-based access control mechanisms and identification/authentication mechanisms
d. Implementation of centrally controlled global protection policies and user-defined/ad hoc protection policies
e. Control of information use operations (e.g., copy/paste, screen grabbing, printing) including derivative works (e.g., save as, exports)
f. Control of information content operations (e.g., view, create, modify, delete, destroy) including expiration of content
g. A complete audit trail of information use and content operations as well as information protection policy management operations

DATA_IRM_FR-1-2: Shall perform IRM functions to enhance data protection and potential data compromise detection, which may include one or more of the following:

a. Export of audit data to SIEM and/or UEBA systems for additional analysis
b. Data usage analytics and reporting
c. Interfacing capabilities via APIs to support other monitoring capabilities
d. Multifactor authentication data

SECTION 3 REFERENCES

3.1 CDM Key Cross-References

This section lists the key program artifacts and briefly summarizes each document's purpose, content, and relevance to this Volume Two document.

1. *CDM Technical Capabilities Volume One: Defining Actual and Desired States, Version 1.4 (July 2017)* [1]. This document presents the high-level CDM Architecture, defines CDM Actual and Desired States and describes the relationship between the CDM program and the NIST CSF and RMF.
2. *CDM Data Model Document, Version 3.8.1 (March 2020)* [2]. This document provides descriptions and specifications of CDM data elements as they relate to CDM Capabilities. This document is a companion artifact to the CDM LDM and it clarifies its development, intent, and usage.
3. *CDM Dashboard Physical Data Model ("Dashboard Data Target, Release 1.0")* [4]. This artifact enumerates the physical implementation of the program's LDM (i.e., the common data schema). The common data schema is implemented within the DHS PMO selected platform for the data store, Elasticsearch at CDM Architecture Layer C.
4. *CDM Integrated Data Dictionary, Version 2.1 (August 2019)* [5]. This dictionary is the authoritative source for key terms and definitions for the CDM Program's architecture and associated critical acquisition artifacts.
5. *CDM Logical Data Model (March 2020)* [3]. This is the CDM LDM for the program. This artifact, in combination with the *CDM Data Model Document*, is the principal artifact for conveying data requirements of the program.
6. *CDM Requirements Management System (RMS)* [8]. This DHS-hosted online system is the authoritative source regarding the program's continuously updated and maintained functional baseline.
7. *CDM Operational Requirements Document (ORD), Version 3.0, (February 2017)* [9]. This document builds upon the mission needs statement of the program and provides the operational requirements and KPPs for the CDM system.

3.2 General References

[1] "CDM Technical Capabilities Volume One: Defining Actual and Desired States," Version 1.4, July 2017.
[2] "CDM Data Model Document, Version 3.8.1," March 2020.
[3] "CDM Logical Data Model, Version 3.1," June 2019.
[4] "CDM Dashboard Physical Data Model (CDM Data Target)," not yet published.
[5] "CDM Integrated Data Dictionary, Version 2.1," August 2019.
[6] U.S. Department of Defense Deputy Chief Information Officer, "Department of Defense Architecture Framework (DoDAF) Version 2.02, AV-2: Integrated Dictionary," August 2010.
[7] "Continuous Diagnostics & Mitigation (CDM) Program" (available at https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program).
[8] "CDM Requirements Management System (RMS)," Online system, continuously updated.
[9] "CDM Operational Requirements Document (ORD)," Version 4.0, March 2019.
[10] Public Law 93-579, as codified at 5 U.S.C. 552a, "The Privacy Act of 1974 (As Amended)," n.d. (available at https://dpcld.defense.gov/Portals/49/Documents/Privacy/pa1974.pdf)
[11] 32 Code of Federal Regulations Part 2002, Executive Order 13556, "Controlled Unclassified Information," 4 November 2010.
[12] NIST FIPS 140-2, "Security Requirements for Cryptographic Modules," 3 December 2002.
[13] NIST FIPS 140-3, "Security Requirements for Cryptographic Modules, Information Technology Laboratory NIST," 22 March 2019.
[14] U.S. General Services Administration, "Internet Protocol Version 6 (IPv6)," n.d. (available at https://www.gsa.gov/technology/technology-products-services/it-security/internet-protocol-version-6-ipv6)
[15] NIST SP 800-119, "Guidelines for the Secure Deployment of IPv6," December 2010.
[16] NIST, "Estimating IPv6 & DNSSEC External Service Deployment Status-Background and Methodology" (available at https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov).
[17] Section 508 of the Rehabilitation Act of 1973, codified at 29 U.S.C. §794d, as amended .
[18] NIST, "Common Platform Enumeration (CPE)," Online dictionary, continuously updated.
[19] The MITRE Corporation, "Common Vulnerabilities and Exposure (CVE)," Online list, continuously updated.
[20] NIST, "National Vulnerability Database (NVD)," Online repository, continuously updated.
[21] NIST FIPS 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013.
[22] NIST SP 800-53 (Revision 4), "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.
[23] CISCO, "Introduction to CISCO IOS NetFlow," May 2012.
[24] NIST, "Common Weakness Enumeration (CWE)," Online list, continuously updated.
[25] U.S. Federal Government, "Federated Identity, Credential, and Access Management (FICAM)," 2 December 2011.
[26] The Committee on The Judiciary, "Federal Rules of Evidence," 1 December 2019.
[27] "CDM Agency-Wide Adaptive Risk Enumeration (AWARE) Technical Design Document," Version 1.2, 16 October 2019.
[28] International Telecommunications Union, "Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks (X.509 ITU-T)," 12 February 2002.
[29] Internet Engineering Task Force, "RFC 7642, System for Cross-domain Identity Management (SCIM): Definitions, Overview, Concepts, and Requirements," September 2015.
[30] NIST, "Cryptographic Algorithm Validation Program (CAVP)," 5 October 2016.
[31] The MITRE Corporation, "ATT&CK, Content version 6.3," 9 March 2020.

[32] Organization for the Advancement of Structured Information Standards, “eXtensible Access Control Markup Language (XACML) 3.0,” 22 January 2013.
[33] Organization for the Advancement of Structured Information Standards, “Security Assertion Markup Language (SAML) 2.0,” 15 March 2005.

APPENDIX A: ACRONYMS

Acronym	Definition
AAL3	Authenticator Assurance Level 3
ABAC	Attribute-Based Access Control
ACL	Access Control List
AEC	Application Execution Control
API	Application Program Interface
APL	Approved Product List
AWARE	Agency-Wide Adaptive Risk Enumeration
BOUND	Boundary Protection
CA	Certificate Authority
CAT	Category
CAVP	Cryptographic Algorithm Validation Program
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CFR	Code of Federal Regulations
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CMDB	Configuration Management Database
CMN	Common
CONOPS	Concept of Operations
CPE	Common Platform Enumeration
CSF	Cybersecurity Framework
CSM	Configuration Settings Management
CSV	Comma-Separated Value
CUI	Controlled Unclassified Information
CVE®	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring Standard
CWE	Common Weakness Enumeration
CybOX™	Cyber Observable eXpression
DAC	Discretionary Access Control
DBS	Design and Build in Security
DEFEND	Dynamically Evolving Federal Enterprise Network Defense
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DMD	Data Model Document
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DPM	Data Protection Management
DTLS	Datagram Transport Layer Security
EDR	Endpoint Detection and Response
EMM	Enterprise Mobility Management
ESN	Electronic Serial Number
ETL	Extraction-Transformation-Load
FICAM	Federated Identity Credential and Access Management
FIPS	Federal Information Processing Standard
FIRR	Federal Incident Response Requirements
FISMA	Federal Information Security Management Act
FR	Functional Requirement
FRD	Functional Requirements Document
FY	Fiscal Year
GPS	Global Positioning System

Acronym	Definition
GSA	General Services Administration
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HWAM	Hardware Asset Management
ICAM	Identity, Credential, and Access Management
ID	Identification
IdAM	Identity and Access Management
ILM	Identity Lifecycle Management
IoA	Indicator of Attack
IoC	Indicator of Compromise
IP	Internet Protocol
IPSec	Internet Protocol Security
IRM	Information Rights Management
IT	Information Technology
JSON	JavaScript Object Notation
KPP	Key Performance Parameter
LDM	Logical Data Model
MAC	Mandatory Access Control Media Access Control
MACSec	Media Access Control Security
MAS	Multiple Award Schedule
MAV	Mobile Application Vetting
MDR	Master Device Record
MEID	Mobile Equipment Identifier
MIR	Master Incident Record
MNGEVT	Manage Events
MSR	Master System Record
MTD	Mobile Threat Defense
MUR	Master User Record
NAC	Network Access Control
NARA	National Archives and Records Administration
NetFlow	Network Flow
NGAC	Next Generation Access Control
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSM	Network Security Management
NVD	National Vulnerability Database
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OMI	Operate, Monitor, and Improve
OR	Operational Requirement
ORD	Operational Requirements Document
OS	Operating System
OU	Organization Unit
PAM	Privilege Access Management
PAP	Policy Administrative Point
PDF	Portable Document Format
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification

Acronym	Definition
PKI	Public Key Infrastructure
PMO	Program Management Office
POAM	Plan of Action and Milestones
RBAC	Role-Based Access Control
RDP	Remote Desk Protocol
RFS	Request for Service
RMF	Risk Management Framework
RMS	Requirements Management System
RTM	Requirements Traceability Matrix
S/MIME	Secure/Multipurpose Internet Mail Extension
SAOP	Senior Agency Official for Privacy
SCAP	Security Content Automation Protocol
SCIM	System for Cross-domain Identity Management
SCRM	Supply Chain Risk Management
SDLC	System Development Lifecycle
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIN	Special Item Number
SP	Special Publication
SSH	Secure Shell
SSO	Single Sign-On
SSP	System Security Plan
STIG	Security Technical Implementation Guide
STIX™	Structured Threat Information eXpression
SWAM	Software Asset Management
SWID	Software Identification
TAXII™	Trusted Automated eXchange of Indicator Information
TLS	Transport Layer Security
U.S.C.	United States Code
UEBA	User and Entity Behavior Analytics
UID	Unique Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Coordinated Time
VPN	Virtual Private Network
VUL	Vulnerability Management
WLAN	Wireless Local Area Network
XACML	eXtensible Access Control Markup Language
XCCDF	eXtensible Configuration Checklist Description Format
XML	eXtensible Markup Language