CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

Technical Capabilities

Volume Two: Requirements Catalog

2020

Cybersecurity and Infrastructure Security Agency (CISA)
Cybersecurity Division

RECORD OF CHANGES

Table of Changes

Version Number	Date	Revised by	Sections
1.0	7/18/2017	PMO	All
1.4	05/11/2018	PMO	Integrate CDM Phase 4 “How is data protected?” requirements.
2.0	6/30/2020	PMO	All; includes new/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)”

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. Therefore, 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 United States (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, to include as part of DEFEND integration contractor efforts post-award and for ongoing updates to the General Services Administration (GSA) Multiple Award Schedule Information Technology Category (MAS IT) 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 the program as “Capabilities”) into the solutions deployed on Agency networks. Figure 1 shows each capability is aggregated into a Capability Area (formerly known as “phases”) that has an underlying security focus area (devices, users, networks, and data).

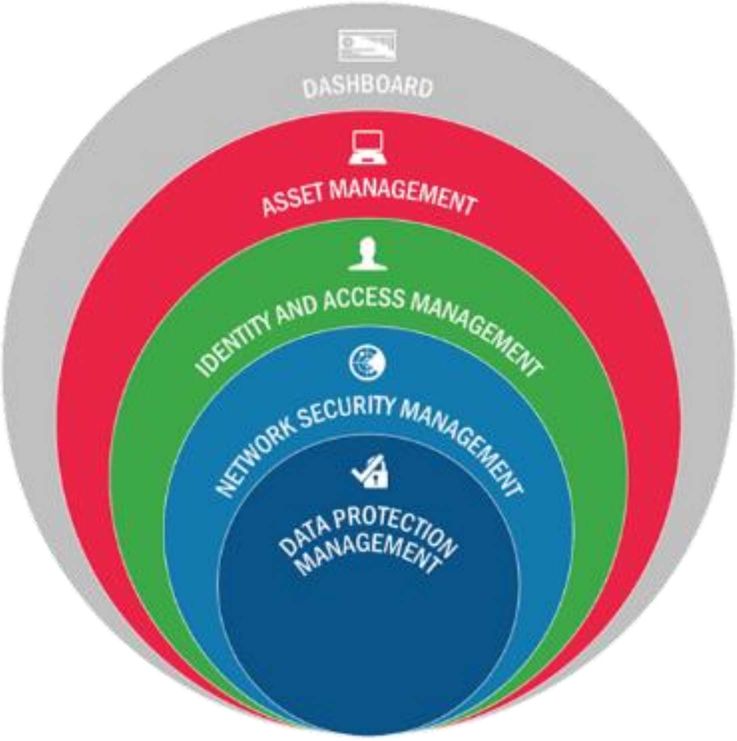

DASHBOARD
ASSET MANAGEMENT
IDENTITY AND ACCESS MANAGEMENT
NETWORK SECURITY MANAGEMENT
DATA PROTECTION MANAGEMENT

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), and Enterprise Mobility Management (EMM).
- **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). The IDAM Capability Area provides identity proofing and authentication aspects under identity management. IDAM supports the use, maintenance, and protection of sensitive resources (e.g., data, systems, etc.).
- **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. Network Security Management consists of the following complementary capabilities:
    - **Boundary Protection (BOUND)** – Capability that provides network boundary protections that support the network security management key program area. Specifically, BOUND is entrusted with providing network security capabilities to prevent and mitigate any unauthorized network, 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 also 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 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 document, CDM Technical Capabilities Volume Two: Requirements Catalog (henceforth referred to simply as “Volume Two”), 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 (3.1 CDM Key Cross-References), 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] This document will be republished on a yearly cadence based upon iterative changes and requirements development work contained within the CDM program’s Requirements Management System (RMS), which is continuously ongoing.

1.1.1 Applicability

Volume Two captures functional requirements for the CDM program[2]. The intent of this document is to align capability functions to operational requirements and Key Performance Parameters (KPPs) in the CDM Operational Requirements Document (ORD). Volume Two has two principle use cases. First and foremost, as an engineering baseline, provided to CDM integrators, for use during CDM solution development within contract activities (e.g., using the RFS process). Integrators use these 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 case, Volume Two is distributed to tool/vendor stakeholders for curating the CDM APL, which contains proposed technologies that are expected to meet some set of CDM requirements. Unless otherwise specified, all requirements apply to the CDM solutions being implemented, this is the functional baseline. Any deviations constitute a baseline change and must be sought 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) 2020 update includes the following:

1. Enterprise Mobility Management (EMM) capability – New capability for CDM, requirements tailored to explicitly manage mobile devices.
2. Promotion of the Network Access Control (BOUND-NAC) capability – New sub-capability within BOUND for CDM. Renamed the former “Network Access Protection” sub-function to NAC, consistent with industry terminology, and promoted as its own sub-capability (BOUND-NAC). Refined the sub-capability by adding new functionality and requirements based on lessons learned in pilot activities and technical research.

[1] OMB Memorandum M-20-04. “Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements.” https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf.

[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 exception are non-functional requirements included to ensure highly desirable properties of the CDM solution that cannot be captured in other artifacts yet.

3. Modernization of COMMON, HWAM, CSM, and VUL capabilities – Capabilities were updated based upon industry and program changes. New style was applied to capability sections to enhance clarity of requirements and better define engineering scope for agencies and CDM integrators.

1.2 Scope

As an 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-D), but the current scope is limited to requirements related to the capabilities that reside in Layer A (i.e., CDM tools/sensors sub-system) of the CDM Architecture. 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 of the Program Management Office's (PMO's) control and are not explicitly defined in this document. The primary example of this occurs 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).

Finally, other items out of scope of this FRD include:

- Formal program definitions, terms (See Section 3.1, CDM Key Cross-References, *CDM Integrated Data Dictionary*)
- Specification-level data requirements (See Section 3.1, *CDM Data Model Document* 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 Approved Products List 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/processes that are intended to facilitate CDM Dashboard data integration (i.e., CDM Layer-B tools, technologies, or requirements)

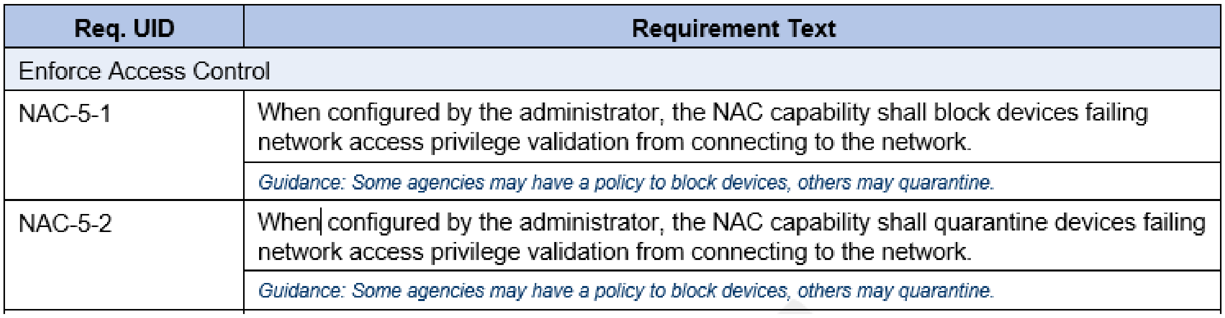
1.3 Style

As previously mentioned, this FRD is written agnostic of Agency-specific needs or requirements as those inputs are expected to be solicited during the decomposition/derivation process that results in the RTM. Appropriately, the CDM PMO employs a very generic, but consistent, set of verbs and nouns to leave solutions engineering activities unconstrainted (i.e., Agency needs elicitation, requirements decomposition/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 principle 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 need(s) provided that 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 Applicability).

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/sensors that are acquired to support those capabilities. Common requirements should be interpreted as additional requirements for every capability, and as a general principle, common requirements are not duplicated or contradicted within each capabilities' specific requirements.

As a result of the CDM program modernizing its requirements, a new style of requirements was introduced in FY2020 that provides greater engineering clarity and direction. This style features a new numbering scheme (with optional functional groupings), a more dictated sentence structure, and utilizes supplemental guidance statements that are designed to convey more clarity on the requirement to assist in engineering activities.[3] Figure 2 shows an example of this 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 2. New Functional Requirement 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. During this modernization effort, the previous style (employed in May 2018) will coexist in the programs baseline with this revised style. As such, certain capability sections (e.g., Capabilities under DPM) do not follow the model illustrated above and may

[3] Guidance statements are purely for situational awareness and clarifying intent, they are not to be used directly as requirements. Program requirements all follow the same directive statement: "Shall".

contain both operational and functional requirements. These capability sections will be converted to the FRD model over a period of time, based upon future requirement development activities.

SECTION 2 CDM CAPABILITIES

2.1 Common Requirements

The requirements in this section are common, mandatory, and are 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.
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-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 program interfaces (APIs).
	Guidance: The CDM PMO intends to have interoperability between CDM sub-systems and/or capabilities to occur over well defined, open (i.e., non-proprietary) interfaces and protocols (e.g., Internet Protocol (IP), Hypertext Transfer Protocol Secure (HTTPS), etc.) that are sustainably supported by industry (e.g., RESTful APIs). Example of standard formats include but are not limited to JavaScript Object Notation (JSON), Extensible Markup Language (XML), and comma separated value (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.)

Req. UID	Requirement Text
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.
	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 Logical Data Model (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 Logical Data Model (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 sub-system.
	Guidance: This is a key performance parameter that ensures any required data ingested in the dashboard is less than or equal to 72 hours from its source.
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 [12] has been superseded by FIPS 140-3 [13], 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 [10], acquisition sensitive information, Controlled Unclassified Information (CUI) [11], 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 [12] has been superseded by FIPS 140-3 [13], effective September 201. 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 [10], acquisition sensitive information, CUI [11], 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 maintain the data currency requirement of 72 hours or less for CDM-required information to be reported to the CDM Agency Dashboard while scaling to support user and device growth rates defined by the agency or 25% above the current user and device baseline inventories, whichever is higher.
	Guidance: The intent of this requirement is to ensure the CDM solution can accommodate a moderate amount of user/device growth and still achieve performance requirements regarding data completeness and timeliness. Capacity growth is a 5-year projection based upon 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 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:

- Passive detection tools
- Tools to interrogate network infrastructure to detect devices
- Active scanning tools
- Tools that provide packet filtering for device identification

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 / 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 device's authorization status.

Req. UID	Requirement Text
	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 / Unauthorized status indicate whether devices are approved / 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/detected by the HWAM capability.
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/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 / physical data models, data requirement documents). Reported inventories are produced for CDM architecture consumption (e.g., CDM federal/Agency Dashboards). Authorized / Unauthorized status indicate whether devices are approved / unapproved, based on an agency policy.

2.2.2 Software Asset Management (SWAM) Capability

The SWAM capability discovers software installed on managed network hardware devices. Since unauthorized software may be vulnerable and exploited as a pivot to other network assets, there is a need for unauthorized software to be removed or managed. In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings. Malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate throughout the enterprise.

SWAM establishes and maintains a software inventory, unique identifiers for software, and other properties such as the manager of the software.

SWAM also establishes and maintains the actual inventory of all software in accordance with data currency requirements, along with information needed to assess the risk to and physically locate the software.

The capability to maintain and update the software inventory needs to enable decentralized administration, using appropriate access and audit controls, to ensure that only authorized personnel with appropriate privileges can modify authorized inventories, and only for software for which they are accountable.

The authorized software inventory baseline is established through some process involving actual inventory data and business rules that determine assignment of default responsibility. Data in the authorized software inventory baseline should be validated continuously through automated software discovery. Manual processes, such as assigning software to the baseline, are expected to integrate with and be supported by automated processes.

2.2.2.1 SWAM Operational Requirements

SWAM _OR-1-1: Shall identify and track software products that are on the device for each hardware device (physical and virtual) on the network within Agency system boundaries, authorization status, and who (by individual, access group, or organization) manages each software product.

SWAM_OR-1-2: Shall allow manual or batch creation of authorized software data (e.g., through integration with external asset information repositories or through business rules).

2.2.2.2 SWAM Functional Requirements

This capability requires CDM solutions to collect information about attributes in the organization unit (OU) and FISMA containers and the MDR. This capability is related to CSM to ensure that software configuration settings are correctly maintained. This capability also is related to DBS to understand the provenance of software and the risk associated with the development and acquisition of software components. If cryptography is used, this capability is related to BOUND-E. This capability is related to DATA_SPIL when the breach/spillage is related to software.

SWAM_FR-1-1: Shall:

a. Provide a unique identifier (e.g., Common Platform Enumeration [CPE], Software Identification Tags) for each software product that is used to identify instances of installed software products and components, including version number, across devices on the network.
b. Identify and collect software inventory information on Agency defined and scoped devices on the network on a scheduled and ad hoc basis as specified by authorized users.
c. Collect additional data (e.g., software components, component digital fingerprints) for managed and properly configured devices, with credentials sufficient to validate actual inventory data.
d. Document and record software inventory information, including product name, owner/manager, and operational status.

SWAM_FR-1-2: Should execute detect/protect for:

a. Malware (including, as configured, all on whitelisted software, and software not behaving as expected) at a rate comparable to existing anti-virus products, and provide a means for removing malware in time to prevent it from executing.
b. Whitelist changes and software installation actions.
c. Unauthorized software execution by blocking based on an authorized software list specific to each hardware device. At a minimum, resident executables must be blocked.

2.2.2.3 SWAM Tool Functionalities

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

- Blacklisting tools
- Whitelisting tools
- Software version scanning tools
- License management tools

2.2.3 Security Configuration Settings Management (CSM) Capability

The security configuration settings management (CSM) capability reduces misconfiguration of assets, including misconfigurations of devices (physical and virtual machines), as well as associated operating systems 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.[6, 7]

The CSM capability interrogates targeted devices for compliance against security configuration benchmarks (CSM benchmarks[8]). CSM benchmarks consist of the 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.[9]

CSM also supports Agency extensions or exceptions (an authorized difference with the justification for the difference from the benchmark) to facilitate tailoring of CSM benchmarks to agency policy and risk thresholds. 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 CDM Program is supporting critical settings from the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)[10] as the de-facto standard for identifying configuration settings that impact a system’s overall risk posture. STIG CAT I findings are utilized in the current (v1.x) Agency-Wide Adaptive Risk Enumeration (AWARE) scoring algorithm. STIG CAT I configuration items are generally viewed as describing key settings on software (inclusive of operating systems) where deviation from the desired state present severe, potentially exploitative conditions that can directly result in a loss of confidentiality, availability, or integrity.

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

- Unified Endpoint Management Tools

[6] 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”.

[7] See https://attack.mitre.org/tactics/TA0008/

[8] Refer to the Program’s Data Dictionary (AV-2) for the formal definition of a security configuration benchmark.

[9] See Continuous Diagnostics and Mitigation (CDM) Agency-Wide Adaptive Risk Enumeration (AWARE) Technical Design Document, Version 1.2, October 16, 2019.

[10] https://nvd.nist.gov/ncp/repository [Select: “Defense Information Systems Agency” under “Authority”]

- Endpoint / Network Device Management Tools
- Vulnerability Assessment Tools
- Security Content Automation Protocol (SCAP) configuration assessment tools

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 4. 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[11].
	Guidance: Installed software also includes operating systems that are installed on the targeted device.
CSM-1-2	The CSM capability shall maintain a unique identifier 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.

[11] 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 and/or security baseline (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 on 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 and/or security baseline (applications, OS, etc.) of a device. This includes differences that provide greater protection or reduce risk further than the CSM benchmark.
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 baselines 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 baselines" 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 baseline 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.

Req. UID	Requirement Text
CSM-4-4	The CSM capability shall restrict which administrators can modify CSM baselines on an individual security baseline basis, based on agency policy.
	Guidance: “CSM baselines” 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 baseline 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 CSM baseline 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 an at-large security baseline for the device. A security baseline 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, CSM baselines assigned to devices shall also assign the baseline’s associated CSM benchmarks to the devices for scanning.
	Guidance: “CSM baselines” 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 baseline for a device.
CSM-6-3	The CSM capability shall maintain a unique identifier for each CSM baseline on the network.
	Guidance: “CSM baselines” 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 baseline for a device.
CSM-6-4	The CSM capability shall track changes made to any created CSM baseline.
	Guidance: “CSM baselines” 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 baseline for a device.
CSM-6-5	The CSM capability shall display changes in CSM baselines by date and by administrator who made the change.
	Guidance: “CSM baselines” 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 baseline 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).

Req. UID	Requirement Text
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.
	Guidance: 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 operating systems 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 (VUL) Management Capability

The CDM vulnerability management (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[12]]) 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 (CVE)s. 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

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

- **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-positives scenarios (e.g., maximizing timely and accurate detection and reporting of vulnerabilities as they are remediated by the Agency)
- **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 Design and Build in Security (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:[13]

- Vulnerability scanners (network or agent based)

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.

[13] These are a general set of technologies used to drive requirements developments against key functionality presented by industry. They are not to be interpreted as requirements, which are represented in “shall” statements.

Table 5. 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.
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 mis-characterizing 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.

Req. UID	Requirement Text
	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%.
	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: (i) 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 (ii) 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 (a) 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 (b) the VUL capability vulnerability database and to make sure all of the CVEs identified in (a) 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[14] 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.

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

Req. UID	Requirement Text
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.
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.

Req. UID	Requirement Text
	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.), and • 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.
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
	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). *Examples of meta data 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*

2.2.5 Enterprise Mobility Management Capability[15]

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 whitelisting/blacklisting
- Disabling access to public app stores and other carrier pre-installed apps
- 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

[15] References:

- NIST Special Publication (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 v3.1.

policy settings. This information is needed to provide a view of the network health and can be tracked over time to determine if 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:[16]

- Enterprise Mobility Management tools
- Unified Endpoint Management tools
- Asset management tools
- Mobile Device Management tools
- Mobile Application Management tools

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

[16] 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.

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. 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 blacklist 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 blacklisted mobile application.
	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 whitelist 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 non-whitelisted mobile application.
	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.

Req. UID	Requirement Text
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.
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 upon 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")

Req. UID	Requirement Text
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.
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.
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.
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

Req. UID	Requirement Text
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.
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: • Operating system (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.

Req. UID	Requirement Text
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
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 whitelist of mobile devices by: • Vendor and model or • An agency-defined unique identifier
	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 "unique identifier" 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.

Req. UID	Requirement Text
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.*
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.

Req. UID	Requirement Text
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.

2.3 Identity and Access Management (IDAM) Capability Area

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, ensuring that they have been properly identified, vetted, trained, and authenticated.

IDAM capabilities collect both actual state and desired state information. The actual state is compared with the desired state using a Policy Decision Point (PDP). The PDP represents the desired state through machine readable policies that the PDP can use to detect defects.

The four component capabilities are:

1. Trust determination for people granted access (TRUST). TRUST functional requirements relate to the identity origination and background investigations performed on the user.
2. Security-related behavioral training (BEHAVE).[17] BEHAVE functional requirements relate to the training and certifications required and completed.
3. Credentials and authentication (CRED). CRED functional requirements track the users’ credentials and the systems and accounts assigned to which the user.
4. Management and control of account and access privileges (PRIV). PRIV functional requirements identify systems to which users have access and their privileges on those systems

2.3.1 TRUST Requirements

The 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 systems and credentials, including user, system, and users with elevated privileges and special security roles. This includes the requirement that the vetted trust level is properly monitored and renewed per Agency policies and applicable statutes.

The primary attributes that will be looked at within the trust capability are that the background investigations and any related determinations are “current” (as specified in the Federal Identity, Credential, and Access Management [FICAM] roadmap) according to the “currency” criteria of the Agency:

[17] Security-related behavioral training includes any role-based training needed that is associated with sensitive information being processed, transmitted, or stored.

- Security clearance determination (if applicable)
- Suitability determination
- Fitness determination

Collecting data associated with the level of trust granted to a user, the level of trust required for an attribute, actual attributes for which the user is assigned or authorized, and other locally defined policy for attributes and TRUST levels will provide measurable data for the performance of automated security checks. These security checks will provide the basis for automating the monitoring, reporting, and prioritizing of trust deficiencies, including those specific to sensitive information, within an Agency's cyber environment.

The TRUST capability will help ensure that every user meets the required trust level of any assigned attribute, is periodically rescreened to revalidate trustworthiness, and is not assigned to incompatible attributes that violate an Agency's policies.

2.3.1.1 TRUST Operational Requirements

TRUST_OR-1-1: Shall:

a. Employ an established screening/indoctrination process before granting access to various levels of sensitive information (including privacy data).

b. Make key trust level authorization attributes available to the systems and processes that monitor/enforce access.

c. Have security checks that provide the basis for automating the monitoring, reporting, and prioritizing of trust deficiencies in an Agency's cyber environment.

d. Provide, to control systems and processes that monitor/enforce access, key TRUST attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility, an account on a system, or access to information at any level of sensitivity.

2.3.1.2 TRUST Functional Requirements

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers and the Master User Record (MUR). This capability is related to BOUND-F to support access control decisions for access to facilities, systems, and information at any level of sensitivity.

TRUST_FR-1-1: Shall:

a. Collect and report TRUST information on all users.

b. Capture the granted trust level for each authorized user.

c. Capture the required operational trust level for each user.

d. Determine when a user issued a credential does not meet trust level requirements and when that user's trust level has expired.

2.3.1.3 TRUST Tool Functionalities

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

- Audit reporting
- Policy management

2.3.2 BEHAVE Requirements

The BEHAVE capability documents that authorized users exhibit appropriate security-related (e.g., role-based) behaviors. 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. Agencies have an increased risk when any user is granted access to facilities, systems, and information at any level of sensitivity without the appropriate security training, demonstrated skill specialty knowledge, or certification. These users may have been granted access to resources or sensitive data without completing proper security-related documentation or training, may have ineffective training, or may not have been assigned the proper training for the access. Poorly trained users can 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.

Collecting data associated with completed training, security-related behavior documentation required for an attribute, and actual attributes for which the user is assigned or authorized 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 security-related behavior deficiencies, including deficiencies specific to sensitive information, within an Agency’s cyber environment. Additionally, the collected data can also be used as a decision factor when granting access to sensitive information.

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 facilities, systems, and information at any level of sensitivity. The BEHAVE capability can also be leveraged to ensure that authorized users exhibit appropriate behaviors for handling sensitive information and meeting annual reporting requirements for training related to sensitive information, such as PII.

2.3.2.1 BEHAVE Operational Requirements

BEHAVE_OR-1-1: Shall:

a. Validate the existence of Agency training policies and report on their enforcement. Agency training policies shall document how long a training/knowledge/certification activity is valid before it expires, and the user is required to repeat the training/knowledge/certification.

b. Make reports of successful completion of required training/knowledge/certification available to the systems and processes that can monitor/enforce access.

c. Collect data associated with completed training/knowledge/certification and security-related behavior documentation required for security-related behavior requirements for which the user is assigned or authorized in order to provide measurable data elements for the creation of automated security checks.

d. Provide, to control systems and processes that monitor/enforce access, key BEHAVE attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility, an account on a system, or access to information at any level of sensitivity.

BEHAVE_OR-1-2: Should:

a. Utilize automated security checks to provide the basis for automating identifying, monitoring, reporting, prioritizing, reviewing, and correcting security-related behavior deficiencies in an Agency's cyber environment.

b. Define appropriate grace periods for training/knowledge/certification associated with each security-related behavior requirement.

2.3.2.2 BEHAVE Functional Requirements

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers and the MUR. This capability is related to BOUND-F to support access control decisions for access to facilities, systems, and information at any level of sensitivity. This capability is also related to MNGEVT and OMI when behavior events related to incidents are recorded in the Master Incident Record (MIR) and may influence attribute values in the MUR.

BEHAVE_FR-1-1: Shall:

a. Collect and report BEHAVE information for each authorized user in the Agency.

b. Collect and report security-related behavior indicators for each authorized user in the Agency, which may include training completed, knowledge demonstrated, and/or certification obtained, depending on Agency policy.

c. Support collection, monitoring, and reporting of general security-related training applicable to all users.

d. Support collection, monitoring, and reporting for security-related training based on the roles authorized/assigned to the user.

BEHAVE_FR-1-2: Should:

a. Provide collection mechanisms and/or processes to detect and record/report information to identify when an authorized user does not meet attribute-based security-related behavior requirements, and when an authorized user's security-related behavior requirements have expired.

2.3.2.3 BEHAVE Tool Functionalities

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

- Audit reporting
- Learning management system
- Security-related behavior management

2.3.3 CRED Requirements

The CRED capability reduces the probability of loss in availability, integrity, and confidentiality of data by ensuring that only proper credentials are authenticated to systems, services, facilities, and information at any level of sensitivity. This includes the requirement that credentials are properly monitored and renewed per Agency policy. The capability is intended to ensure that credentials for access are assigned to, and only used by, authorized users or services that require that access to perform their specific job functions.

The CRED capability provides an Agency insight into risks associated with weaknesses in its credential management. The CRED capability collects data associated with the credentials issued to a user, the credential type required for an attribute, actual attributes the user is assigned or authorized, and the locally defined policies for authentication, in order to provide measurable data elements for the creation of automated security checks. These security checks provide the basis for automating the monitoring, reporting, and prioritizing of credential and authentication deficiencies, including those specific to sensitive information, within an Agency’s cyber environment.

CRED capability will help ensure that every user can be authenticated appropriately for access to facilities, systems, and information at any level of sensitivity. The capability will also provide insight into whether authentication, reissuance, and revocation policies are incurring more risk than deemed acceptable by the Agency.

2.3.3.1 CRED Operational Requirements

CRED_OR-1-1: Should:

a. Employ an approved process for issuing different credential types and defining authentication requirement policies for access to various facilities, systems, and information at any level of sensitivity.

b. Provide, to control systems and processes that monitor/enforce access, key CRED attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility, an account on a system, or access to information

c. Continuously monitor key outputs from the credential issuance and authentication definition processes to detect when a credential or authentication action deviates from established standard(s).

d. Verify that all authentication mechanisms deployed on in-scope systems across the Agency implement the appropriate authentication policy.

CRED_OR-1-2: Shall:

a. Verify that all credential types have appropriate expiration, reissuance, and revocation policies.

2.3.3.2 CRED Functional Requirements

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers and the MUR. This capability is related to BOUND-F to support access control decisions for access to systems and information at any level of sensitivity. If cryptography is used, this capability is related to BOUND-E. This capability is related to DATA_SPIL when the breach/spillage is related to improper use of credentials.

CRED_FR-1-1: Shall collect and report CRED information associated with accounts and users, including:

a. Credentials (e.g., X.509 certificates, user identifiers, public/private key pairs) issued to each user employed by the Agency (including contractors).

b. Credential reissuance, revocation, and suspension enforcement mechanisms and their configuration for all applicable credential types.

c. Password complexity enforcement mechanisms and their configuration for all in-scope accounts at the Agency.

CRED_FR-1-2: Shall verify:

a. The authentication mechanisms implemented for every in-scope account at the Agency.

b. Default accounts/passwords are NOT enabled on in-scope systems.

2.3.3.3 CRED Tool Functionalities

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

- X.509 certificates
- Public Key Infrastructure (PKI)
- Identity and access management
- Access certifications
- Authentication mechanisms
- Audit reporting

2.3.4 PRIV Requirements

The PRIV 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. The intent of the capability is to ensure that privileges for both physical and 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.

The PRIV capability collects the privilege rights for all privileged accounts as attributes. Privilege policies can be mapped directly to attributes.

The PRIV capability identifies access beyond what is needed to meet business mission by monitoring and measuring account access privileges, identifying excess privileges, and identifying unneeded accounts. The PRIV capability reduces the risk of the loss of confidentiality, integrity, and availability of data due to the provision of excessive access, including physical access, to people who do not need such access to perform their work.

The PRIV capability helps to ensure that authorizations and accounts do not exceed the privileges required by a user’s attributes. The capability also provides insight into whether access (re)authorization policies are incurring more risk than deemed acceptable by the Agency.

The PRIV capability can also provide insight by compare business responsibilities, rules, and policy to ensure that access to sensitive information, such as PII, is being properly managed and controlled. When privacy data is involved, this insight can assist in meeting requirements associated with consent, collected information, privacy notice, usage, retention, and refresh and synchronization cycles.

2.3.4.1 PRIV Functional Requirements

This capability will require CDM solutions to collect information about attributes in the OU, FISMA, and MUR. This capability may interact with BOUND-F to manage and control access decisions (e.g., in BOUND-F) for systems and information at any level of sensitivity. This capability is related to DATA_SPIL when the breach/spillage is related to misuse of or improper privileges. This capability is related to DATA_DLP when the data protection relies on restricting privileges.

PRIV_FR-1-1: Shall collect and report:

a. PRIV information on privileged and non-privileged accounts and users.

b. Physical access authorizations issued to each user employed by the Agency.

c. Account status (restrictions, enablement, revocation, in authorization time window, etc.) implemented for every in-scope account at the Agency.

2.3.4.2 PRIV Tool Functionalities

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

- Identity and access management
- Privileged account management
- Credential management
- Compliance verification

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 Policy Enforcement Points (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 shall 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 National Institute of Standards and Technology (NIST) Cybersecurity Framework. 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 Security Information and Event Management (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 nine 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 Policy Enforcement Point (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**[18] 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.
8. **Report on Policy Compliance** provides reports of interest, based on NAC logs, to assess events.

Figure 3 is a block diagram showing the relationship among the NAC functions.

[18] See CDM AV-2: “Device Type”

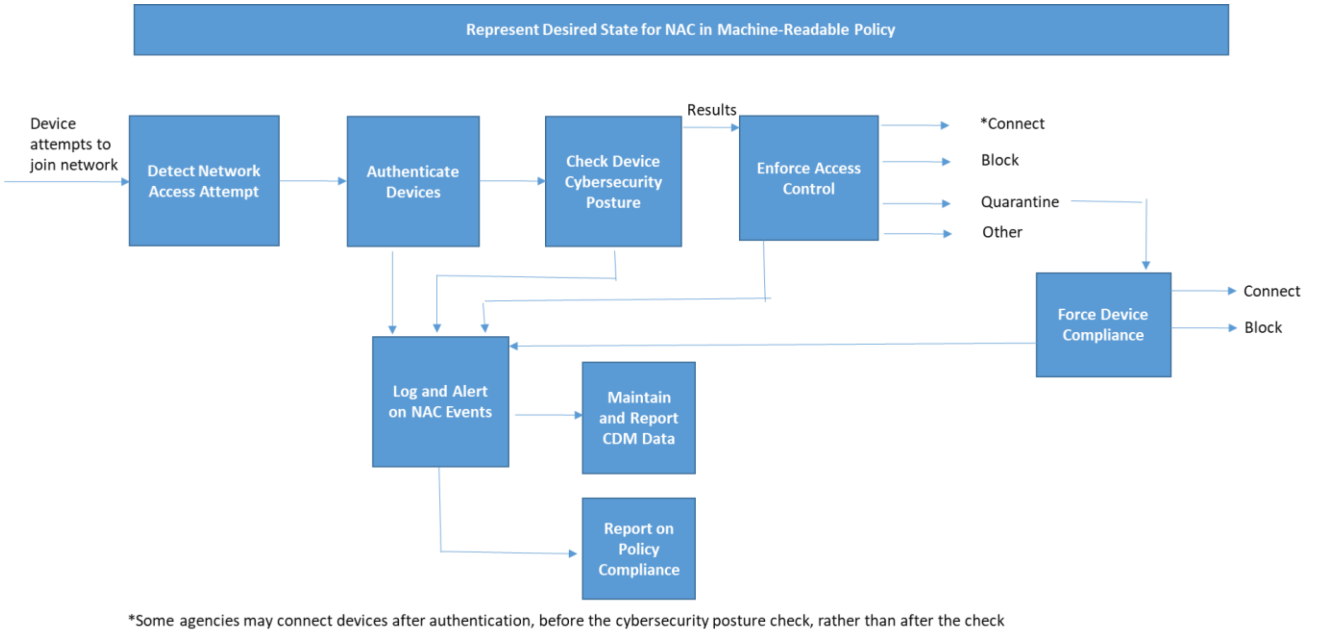

Represent Desired State for NAC in Machine-Readable Policy
Device attempts to join network
Detect Network Access Attempt
Authenticate Devices
Check Device Cybersecurity Posture
Results
Enforce Access Control
*Connect
Block
Quarantine
Other
Force Device Compliance
Connect
Block
Log and Alert on NAC Events
Maintain and Report CDM Data
Report on Policy Compliance
*Some agencies may connect devices after authentication, before the cybersecurity posture check, rather than after the check

Figure 3. 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:

- Network Access Control technologies (implementing network control and/or agents)
- Identity and access management tools that integrate/implement with a control plane (to restrict or remove devices from the network)
- Passive and active asset management detection and scanning tools, including unified/enterprise endpoint management tools (e.g., HWAM capability)
- Network segmentation tools/capabilities
- Integration with other tools
  - SIEM
  - Firewalls
  - Certificate generation tools (e.g., X.509 certificates, Public Key Infrastructure (PKI))
  - Key Management Orchestration

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 7 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 7. 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, etc.) 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.
	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 cybersecurity posture gap (CPG) (i.e., defect), which may be incorporated into a NAC capability decision to allow/prevent device access to the network.
Enforce Access Control	

Req. UID	Requirement Text
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.

Req. UID	Requirement Text
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.
	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. MNGEVT utilizes 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

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 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 support 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 be 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: Should 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.[19]

2.4.4.1.4 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.

[19] 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_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 should 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.

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.[20]

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

[20] 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).

2.5 Data Protection Management 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.

DPM focuses on the protection of sensitive (especially privacy) data,[21] which is covered by the following five capabilities:

1. Data Discovery/Classification (Section 2.5.2) describes techniques for the identification, discovery, and classification of data.
2. Data Protection (Section 2.5.3) describes data protection techniques.
3. Data Loss Prevention (Section 2.5.4) describes techniques to minimize the loss of data.
4. Data Breach/Spillage Mitigation (Section 2.5.5) describes techniques for response and recover activities due to data breach/spillage.
5. Information Rights Management (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[22] as the source definition

[21] Privacy data includes Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI), among others.

[22] See https://www.archives.gov/cui/registry/category-list.

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

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.[23]

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: Should 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

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:

[23] Applicable regulations include Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and others.

- **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),[24] 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
- 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:

[24] 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).

- **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 instantiate 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: Should 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-1-2: 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-1-3: 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. Identity and access management (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: Should 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 a brief summary on each document's purpose/content/relevance to this Vol 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 Cybersecurity Framework (CSF) and Risk Management Framework (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 Logical Data Model (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 logical data model (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,* [5]. This dictionary is the authoritative source for key terms and definitions for the CDM Program's architecture and associated critical acquisition artifacts [5].
5. *CDM Logical Data Model (March 2020)* [3]. This is the CDM Logical Data Model (LDM) for the program. This artifact, in combination with the *CDM Data Model Document*, is the principle artifact for conveying data requirements of the program.
6. *CDM Requirements Management System (RMS)* [8]. DHS hosted online system that is 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 key performance parameters 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 & Monitoring (CDM) Program. 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, "The Privacy Act of 1974 (As Amended)".

[11] "Code of Federal Regulations (CFR) Part 2002, Executive Order 13556 "Controlled Unclassified Information"".

[12] NIST FIPS 140-2, "Security Requirements for Cryptographic Modules," December 3, 2002.

[13] NIST FIPS 140-3, "Security Requirements for Cryptographic Modules, Information Technology Laboratory NIST," March 22, 2019.

[14] U.S. General Services Administration, "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".

[17] "Section 508 of the Rehabilitation Act of 1973, codified at 29 U.S.C. §794d, as amended (Section 508)".

[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)," December 2, 2011.

[26] The Committee on The Judiciary, "Federal Rules of Evidence," December 1, 2019.

[27] "CDM Agency-Wide Adaptive Risk Enumeration (AWARE) Technical Design Document, Version 1.2," October 16, 2019.

[28] International Telecommunications Union (ITU), "Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (X.509 ITU-T)," February 12, 2002.

[29] Internet Engineering Task Force (IETF), "RFC 7642, System for Cross-domain Identity Management (SCIM): Definitions, Overview, Concepts, and Requirements," September 2015.

[30] NIST, "Cryptographic Algorithm Validation Program (CAVP)," October 5, 2016.

[31] The MITRE Corporation, "ATT&CK, Content version 6.3," March 9, 2020.

[32] OASIS (Organization for the Advancement of Structured Information Standards), "eXtensible Access Control Markup Language (XACML) 3.0," January 22, 2013.

[33] OASIS (Organization for the Advancement of Structured Information Standards), "Security Assertion Markup Language (SAML) 2.0," March 15, 2005.

APPENDIX A ACRONYMS

Acronym	Definition
ABAC	Attribute-Based Access Control
ACL	Access Control List
API	Application Program Interfaces
APL	Approved Product List
AWARE	Agency-Wide Adaptive Risk Enumeration
BOUND	Boundary Protection
CA	Certificate Authority
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
CPG	Cybersecurity Posture Gap
CSF	Cybersecurity Framework
CSM	Configuration Settings Management
CSV	Comma Separated Values
CUI	Controlled Unclassified Information
CVE®	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring Standard
CWE	Common Weakness Enumeration
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

Acronym	Definition
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoDAF	Department of Defense Architecture Framework
DPM	Data Protection Management
DTLS	Datagram Transport Layer Security
EMM	Enterprise Mobility Management
ESN	Electronic Serial Number
ETL	Extraction-Transformation-Load
FERPA	Family Educational Rights and Privacy Act
FICAM	Federated Identity Credential and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FR	Functional Requirements
FRD	Functional Requirements Document
FY	Fiscal Year
GPS	Global Positioning System
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
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
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
IRM	Information Rights Management
IT	Information Technology
ITU	International Telecommunications Union
JSON	JavaScript Object Notation
KPP	Key Performance Parameter
LDM	Logical Data Model

Acronym	Definition
MAC	Mandatory Access Control
MAC	Media Access Control
MACsec	Media Access Control Security
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
NIST	National Institute of Standards and Technology
NPE	Non-Person-Entity
NSA	National Security Agency
NSM	Network Security Management
NVD	National Vulnerability Database
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
OMI	Operate, Monitor, and Improve
OR	Operational Requirement
ORD	Operational Requirements Document
OS	Operating System
OU	Organization Unit
PDF	Portable Document Format
PDP	Policy Decision Point
PEP	Policy Enforcement Points
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMO	Program Management Office

Acronym	Definition
POAM	Plan of Action and Milestones
RBAC	Role-Based Access Control
RFS	Requests for Service
RMF	Risk Management Framework
RMS	Requirements Management System
RTM	Requirements Traceability Matrix
S/MIME	Secure/Multipurpose Internet Mail Extension
SAML	Security Assertion Markup Language
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
SOAR	Security Orchestration, Automation and Incident Response
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SWAM	Software Asset Management
TLS	Transport Layer Security
U.S.	United States
U.S.C	United States Code
UEBA	User and Entity Behavior Analytics
UID	Unique Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
VUL	Vulnerability Management
WLAN	Wireless Local area Network
XACML	eXtensible Access Control Markup Language
XCCDF	Extensible Configuration Checklist Description Format

Acronym	Definition
XML	Extensible Markup Language