Homeland Security

Continuous Diagnostics and Mitigation (CDM)

Technical Capabilities

Volume Two

Requirements Catalog

Version 1.4

May 11, 2018

Table of Contents

REVISION SUMMARY

Table of Changes

Version Number	Date	Revised by	Section
1.0	7/18/2017	CDM PMO	All
1.4	4/27/2018	CDM PMO	Integrate CDM Phase 4 “How is data protected?” requirements.

I - 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 U.S. Government entities to assess and improve the security posture of an Agency's information systems. These requirements will be used for the CDM solicitations called Dynamically Evolving Federal Enterprise Network Defense (DEFEND) program as well as the Schedule 70 CDM-SIN Approved Product List (APL).

The companion volume (Volume One) "CDM Technical Capabilities - Defining Actual and Desired States" should be used in conjunction with this document.

Since the cybersecurity space is inherently complex, the CDM approach is to address the problem space in phases, as shown in *Figure 1*:

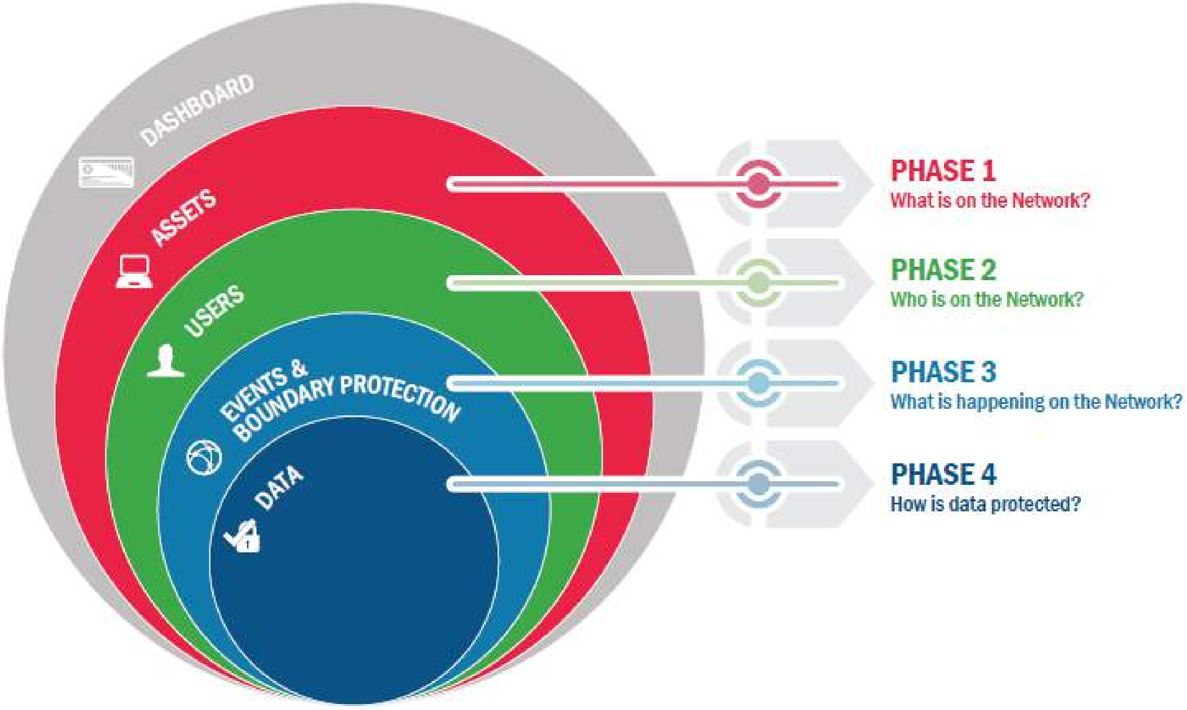

Figure 1: Phases of CDM

The CDM requirements to support these phases are grouped into the following:

1. Requirements to manage "What is on the network?"

2. Requirements to manage “Who is on the network?”
3. Requirements to manage “What is happening on the network?” are decomposed into four sub-areas:
    a. Managing Events (MNGEVT)
    b. Operate, Monitor, and Improve (OMI)
    c. Design and Build in Security (DBS)
    d. Boundary Protection (BOUND) – addressing “How is the network protected?”
4. Requirements to manage “How is data protected?”

I - 1 CDM Key Cross-References

Section II of this document will also reference to the following parts of the Companion:

1. CDM Architecture (Companion I-1)
2. CDM and the Cybersecurity Framework (CSF) (Companion I-2)
3. CDM and the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) (Companion I-3)

Users of this document should be familiar with the contents of the Companion volume.

II - CDM Detailed Requirements

Based on the above enhanced CDM phase definitions, this section describes CDM requirements in terms of those requirements that are common to all phases and then describes the detailed requirements for each area of focus.

While these requirements are for the entire scope of the CDM solution ecosystem, the primary area impacted would be Layer A and B in the CDM Architecture.[1] The CDM Dashboard plays an active role in providing visibility to the outcomes of these requirements and providing the policy orchestration if applicable. There are additional specific requirements to the dashboards (both Federal and Agency) that are managed through the CDM Dashboard-specific development process.

These requirements are also applicable and cover other operational environments, such as cloud and mobile, while the method of execution could differ between environments.

Appendix B provides a mapping of the CDM capabilities to the NIST Cybersecurity Framework (i.e., CSF).

II - 1 Requirements Common to All CDM Capabilities

The requirements in this section are common and mandatory, and apply universally across all CDM capabilities. These requirements are in addition to operational and functional requirements covered in sections II - 2 through II - 5.

References to data protections within Section II are applicable to all types of sensitive information, including privacy data.[2] References to security data protections include protections and safeguards that may be unique to a given type of sensitive information. For example, personally identifiable information (PII) security checks will need to include assessing how the data is allowed to be used.

II - 1.1 Common Actual State

C_AS_OP-1-1: Should interpret all references to security to include data protections and safeguards applicable to all type of sensitive information (e.g., privacy data).

C_AS_OP-1-2: Should interpret all requirements for security capabilities and functionalities to apply to all operational environments.

C_AS_FR-1-1: Shall have a date/time associated with each instance of Actual State information and identify the collection source.

II - 1.2 Common Interoperability

C_Interop_OR-1-1: Shall deliver information to the CDM Dashboard using standardized data structures and/or API (application program interfaces).

[1] Found in CDM Architecture Companion section I-1.1.

[2] Privacy data includes any data subject to the Privacy Act of 1974, as amended. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI) among others.

C_Interop_OR-1-2: Shall support data interchange and sharing between all CDM capabilities using standardized formats.

C_Interop_FR-1-1: Shall receive and collect relevant data via a standard interface and in a standard format to the CDM Dashboard and other solution subsystems using CDM data structure(s), including use of MUR, MDR, MIR, and MSR.[3]

II - 1.3 Common Scaling

C_Scale_FR-1-1: Shall store, process, and provide data for large Federal organizations (using the threshold of up to one million devices) while maintaining adequate timeliness, completeness, and accuracy for applicable capabilities.

C_Scale_FR-1-2: Shall minimize the use of network bandwidth and end point system resources to limit potential impact to mission/business operations.

II - 1.4 Common Securing

C_Secure_FR-1-1: Shall support Federal Information Processing Standard (FIPS) 140-2 approved algorithms to encrypt data, both in transit and at rest, consistent with Federal and Agency policies.

C_Secure_FR-1-2: Should provide source integrity verification for all tool components, such as digital fingerprints for each software file used within the system.[4]

II - 1.5 Common Timeliness and Completeness

C_Time-FR-1-1: Shall support the requirement that attribute information associated with an object is within the 72-hour data currency goal coupled with the 90% coverage goal for all objects.

C_Time-FR-1-2: Shall retain assessment results for an Agency-defined period to enable enterprise security posture reporting and trending.

II - 1.6 Common Grouping

C_Group_OR-1-1: Shall include the mechanism to define risk scores for the difference between actual and desired states (including scores that reflect a reduction in risk) dependent on object context (e.g., Organizational Unit [OU] and Federal Information Security Management Modernization Act [FISMA] container linkage) and the scope of the capability’s attributes.

C_Group-OR-1-2: Shall include the mechanism to define actual state dependent on object context and the scope of the capability’s attributes.

C_Group-OR-1-3: Shall include the mechanism to define the desired state for an object dependent on the object context (e.g., OU and FISMA container linkage) and the scope of the capability’s attributes.

[3] Found in CDM Architecture Companion section I-1.2.4

[4] Dependent on the ongoing formulation of Federal policies directing increased activities for Supply Chain Risk Management (SCRM).

II - 1.7 Common Policy Decision Point

C_PDP_FR-1-1: Shall include Policy Decision Point (PDP) capabilities to support the ingestion of machine-readable policies to measure the actual state against the desired state for ongoing assessment of security controls.

C_PDP_FR-1-2: Shall support the MUR, MDR, MIR, and MSR in conjunction with PDP, specific to the determination of actual versus desired state function of the PDP.

II - 2 Requirements to Manage "What is on the network?"

Managing "What is on the network?" requires the management and control of devices (HWAM), software (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).

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

Note that while the scope of HWAM is to capture the entire Agency "attack surface," the scope of SWAM, CSM, and VUL is specific to the subset of HWAM that is under the accountability and therefore control of the Agency. This is determined by the Agency's overall risk management strategy and as articulated in the Agency's Information Security Continuous Monitoring strategy.

II - 2.1 HWAM Requirements

The HWAM capability discovers IP-addressable hardware on a network.

HWAM establishes and maintains a 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, using appropriate access and audit controls to ensure that only authorized personnel with appropriate privileges can modify authorized inventories, 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.

II - 2.1.1 HWAM Operational Requirements

HWAM _OR-1-1: Shall identify and track hardware devices (physical and virtual) that are on the network, authorization status, and who (by individual, access group, or organization) manages each device.

HWAM_OR-1-2: Shall allow manual or batch creation of Agency approved device data (e.g., through integration with external asset information repositories or through business rules).

II - 2.1.2 HWAM Functional Requirements

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers and the MDR. This capability is related to CSM to ensure that hardware configuration settings are correctly maintained. If cryptography is used, this capability is related to BOUND-E.

HWAM_FR-1-1: Shall:

a. Provide a unique identifier (which may vary by device type) that supports device persistence across network location changes for each device on the network.
b. Identify and collect hardware inventory information on all IP addressable devices on the network on a scheduled and ad hoc basis as specified by authorized users.
c. Collect appropriate data to match actual to authorized Agency approved (i.e., authorized devices) hardware inventory, including when detected and if the device is in desired state.
d. Document and record Agency approved (i.e., authorized devices) hardware inventory information, including device type (e.g., router, workstation, firewall, printer), owner/manager, and operational status.

HWAM_FR-1-2: Should:

a. Collect data to enable staff to locate the hardware devices.
b. Collect additional data (e.g., subcomponents, attached peripheral devices, local account information) for managed and properly configured devices and with credentials sufficient to validate actual inventory data.
c. Detect the type of each hardware device based upon its network behavior.

II - 2.1.3 HWAM Tool Functionalities

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

II - 2.2 SWAM Requirements

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.

II - 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).

II - 2.2.2 SWAM Functional Requirements

This capability requires CDM solutions to collect information about attributes in the 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.

II - 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

II - 2.3 CSM Requirements

The CSM capability reduces misconfiguration of assets, including misconfigurations of hardware devices (including physical and virtual machines, as well as the associated operating system) and software. Cyber adversaries often use automated scanning attacks to search for and exploit assets with misconfigurations, and then pivot to attack other assets.

CSM establishes and maintains security configuration benchmarks, consisting of the acceptable value(s) for each relevant configurable setting for each asset type.

CSM also establishes and maintains the value of the actual settings for each relevant configurable setting for each asset type.

Differences between desired and actual configuration settings represent a change in risk to the system. CSM needs to assign core (using the Federal benchmark) and alternate (using an Agency or system level benchmark) risk scores to each reported configuration setting difference based on relevant factors. The configuration setting’s difference may make the information system more secure (have less risk), which may be accounted for in the risk score determination.

CSM supports managing a change control process that documents Agency extensions or exceptions (an authorized difference with the justification for the difference) to the authorized core Federal benchmarks. CSM also supports the management of configuration settings associated with the specialized capabilities needed for processing or storing of sensitive information such as PII.

II - 2.3.1 CSM Operational Requirements

CSM _OR-1-1: Shall:

a. Create, update, and maintain the security configuration settings benchmarks for target hardware devices and software products, including the Federal core benchmark as well as Agency-specific variations that implement Agency policies.
b. Store, process, maintain, track changes, and distribute security configuration benchmarks, including Agency exceptions (including the justification and compensating countermeasures), as determined by authorized users (with authorization being granted per benchmark).
c. Permit authorized users to select and compose a set of security configuration benchmarks to establish an authorized security configuration baseline for an asset or group of assets.

II - 2.3.2 CSM Functional Requirements

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers, the MDR, and the MSR. This capability is related to HWAM and SWAM to accurately assess hardware and software configuration settings on authorized devices. If cryptography is used, this capability is related to BOUND-E. This capability is also related to MNGEVT to implement auditing on devices. Finally, this capability is related to DBS to ensure implementation of configuration settings baselines provided as part of information system deployment. This capability is related to DATA_SPIL when the breach/spillage is related to improper configuration settings.

CSM_FR-1-1: Should:

a. Support a unique identifier (CCE) for each configuration setting collection across devices on the network.
b. Identify and collect configuration settings (including the actual values) for specific software and hardware products on Agency defined and scoped devices on the network on a scheduled, event-driven, and ad hoc basis as specified by authorized users.
c. Document authorized security configuration settings that are set and managed by authorized users within benchmarks for specific software and hardware products.
d. Enumerate differences from the security configuration benchmark, including differences that provide greater protection or reduce risk further than the benchmark.

II - 2.3.3 CSM Tool Functionalities

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

- Security Content Automation Protocol (SCAP) configuration assessment tools
- CCE assessment tools
- Common Configuration Scoring System (CCSS) tools

II - 2.4 VUL Requirements

The VUL capability discovers vulnerabilities in assets on the network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified. (An information security vulnerability is a deficiency in software that a hacker can use to gain access to a system or network.)

VUL discovers, identifies, and locates known security vulnerabilities in network assets.

Most vulnerabilities are defined by the Common Vulnerabilities and Exposures (CVEs®), though other detectable vulnerabilities may exist that are not in the CVEs® and for which patching may also be an available remedy. Vulnerabilities identified will typically be remediated through the software inventory management function, using updates, patches, plug-ins, and new releases.

II - 2.4.1 VUL Operational Requirements

VUL_OR-1-1: Shall:

a. Update tools in a timely manner to be able detect vulnerabilities that have been identified by the Government CVEs.
b. Discover vulnerabilities on the network using unauthenticated or authenticated methods.

VUL_OR-1-2: Should:

a. Provide text for system administrators to explain clearly and simply how to correct the vulnerability.

II - 2.4.2 VUL Functional Requirements

This capability requires CDM solutions to collect information about attributes in the OU and FISMA containers and the MDR. This capability is related to DBS to discover, identify, and locate other known weaknesses in software applications and source code and the use of Supply Chain Risk Management (SCRM) to support the awareness and understanding of potential exposure to risks associated with the provenance of system components. This capability is related to DATA_SPIL when the breach/spillage is related to software vulnerabilities.

VUL_FR-1-1: Shall:

a. Identify and collect vulnerability information, including time first detected and time remediated, on all IP addressable devices on the network on a scheduled, event-driven, and ad hoc basis as specified by authorized users.
b. Collect appropriate data to map actual vulnerabilities to the on-network hardware and software inventories.

VUL_FR-1-2: Should:

a. Provide complete coverage of the CVEs identified by the National Vulnerability Database (NVD) and equivalent vulnerability information from other useful sources.

II - 2.4.3 VUL Tool Functionalities

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

- Vulnerability scanners
- Web application scanners
- Database scanners
- Import published vulnerabilities

II - 3 Requirements to Manage "Who is on the network?"

Managing "Who is on the network?" requires the management and control of account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE).[5] These four functions have significant interdependencies. The separation of measurements and execution of the controls related to these areas poses a complex set of problems and requires a coordinated effort to properly assess the actual state.

These four functions are briefly summarized below, and the requirements are separately specified later in the TRUST, BEHAVE, CRED, and PRIV sections.

- TRUST validates a person's identity and the degree to which he or she has been vetted.
- BEHAVE identifies that the individual has the proper knowledge and training for the roles he or she is assigned and that he or she remains up to date.
- CRED binds a type of credential or authentication mechanism to an identity established in TRUST with a level of assurance and is used to grant access (physical and logical).
- PRIV establishes the privileges associated with the credential and in turn the individual or service.

II - 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 statues.

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 Federated Identify, Credential, and Access Management [FICAM] roadmap) according to the "currency" criteria of the Agency:

- 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

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

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.

II - 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.

II - 3.1.2 TRUST 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-P and BOUND-F to support physical and logical 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.

II - 3.1.3 TRUST Tool Functionalities

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

- Audit reporting
- Policy management

II - 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.

II - 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.

II - 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-P and BOUND-F to support physical and logical 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 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.

II - 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

II - 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 both physical and logical 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.

II - 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.

II - 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 and BOUND-P to support physical and logical access control decisions for access to facilities, 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.

II - 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

II - 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.

II - 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 and BOUND-P to manage and control logical and physical access decisions (e.g., in BOUND-P and BOUND-F) for facilities, 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.

II - 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

II - 4 Requirements to Manage "What is happening on the network?"

Managing "What is happening on the network?" builds on the CDM capabilities provided by "What is on the network?" and "Who is on the network?" These CDM capabilities include network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. These 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.

"What is happening on the network?" 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 II - 4.1) describes that part of "What is happening on the network?" by focusing on "How is the network is protected?"
- MNGEVT (Section II - 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 II - 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 II - 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.

II - 4.1 Manage BOUND, or "How is the network protected?"

Managing "How is the network protected?" requires capabilities that limit, prevent, and/or allow the removal of unauthorized network connections/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 and addresses physical access systems that limit unauthorized user physical access to Federal Government facilities.

BOUND is categorized into three security capabilities:

- BOUND-F to Manage Network Filters and Boundary Controls
- BOUND-E to Monitor and Manage Cryptographic Mechanisms Controls
- BOUND-P to Monitor and Manage Physical Access Controls

II - 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
- Network Access Protection
- 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.

II - 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. Network Access Protection 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. Network Access Protection policies permit access to a network only if a device is approved to access that network, and is compliant with policies regarding hardware, software, configuration, and patching. For example, a device attempting to connect to a network can be blocked from connecting if the latest security updates are not installed. Network Access Protection also contains functions that can force the patching or upgrading of a device, and then allow connection. Network Access Protection policies describe the device connection actions that are filtered based on rules and policies.

f. 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).

II - 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 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 physical and logical access control decisions for access to facilities, 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. Network Access filtering that implements policy for permitting devices to connect to the network. Network Access filtering is described in terms of the types of devices the policy applies to, authentication method, and device characteristics used to make the connection decision.

f. 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.

II - 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
- Network Access Protection or Control Devices
- Intrusion Detection or Prevention Systems

II - 4.1.2 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

II - 4.1.2.1 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.

II - 4.1.2.2 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:

   – Cryptographic Algorithm Validation Program (CAVP) http://csrc.nist.gov/groups/STM/cavp/standards.html

   – NSA’s Suite B Cryptographic Program https://www.nsa.gov/ia/programs/suiteb_cryptography/.

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 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 musts 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 Service (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.

II - 4.1.2.3 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., 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., MACsec)
- Network-layer (e.g., 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.

II - 4.1.3 BOUND-P Requirements

The BOUND-P capability ensures that personnel and vehicle access through a protected facility boundary is properly authenticated as required by policy, is properly authorized as required by policy, and the events are properly monitored. Physical Access Control Systems (PACS) are the underlying systems that provide policy rules and events to the BOUND-P services for electronically protecting facility access boundaries. “Properly authenticated” means that the individual presented FIPS 201 approved credentials and that a cryptographic validation was performed to verify that the individual is as represented. Credential validation uses only approved algorithms; ensures that cryptographic keys used are supplied by the approved key management system; and ensures that cryptography is applied utilizing the correct network security protocols at the correct layers within the protocol stack.

II - 4.1.3.1 BOUND-P Operational Requirements

BOUND_OR-3-1: Shall integrate with IP-addressable PACS components to support all CDM capabilities.

II - 4.1.3.2 BOUND-P Functional Requirements

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

BOUND_FR-3-1: Shall collect and report information related to

a. Physical boundary authentication for providing identification and authentication of the person requesting access, as well as the validation requirements for identification/ authentication. Boundary authentication is described in terms of the CDM Phase 2 CRED attributes, the authentication mechanism from FIPS 201 (e.g., Personal Identity Verification [PIV] + Biometric [BIO]), and the validation methods (e.g., Certificate Revocation List check) for the certificate attributes outlined for BOUND-E.

b. Boundary authorization to record and describe the policy for authorizing access to the controlled area. Boundary authorization records need to be described in terms of the CDM Phase 2 CRED identity, attributes from the MUR (e.g., CDM Phase 2 BEHAVE, TRUST, and/or PRIV attributes), environmental attributes (e.g., time of day), and/or previous boundary authorization actions.[6]

c. Physical boundary filtering policies determine what access for personnel or vehicles is allowed to a given space or facility. A physical boundary policy is the set of authentication and authorization policies for a boundary, including metadata about that policy.

II - 4.1.3.3 BOUND-P Tool Functionalities

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

- Possession of a valid token
- Identification, authentication (e.g., token with Personal Identification Number)
- Identification, strong(er) authentication (e.g., biometrics)
- “Need-to-know” (e.g., group membership, security clearance) required
- Training/certification (e.g., physical security training specific to the area) required

[6] For example, access to a highly controlled area in a facility can be granted only if the same credential has already been granted access to the facility.

- Movement between less trusted and more trusted areas incorporates previous access control decisions (e.g., moving to a Limited area from a Controlled area is granted only if access to the Controlled area has been granted previously and within a specified time)

II - 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

II - 4.2.1 MNGEVT Operational Requirements

II - 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.

II - 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.

II - 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.

II - 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:
    1. Appropriate audit data that can be used to support security assessment and forensic analysis
    2. Audit records that meet regulatory requirements
    3. 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.

II - 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.

II - 4.2.2 MNGEVT Functional Requirements

II - 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.

II - 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.

II - 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.

II - 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.

II - 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.

II - 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

II - 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

II - 4.3.1 OMI Operational Requirements

II - 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.

II - 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).

II - 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.

II - 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.

II - 4.3.2 OMI Functional Requirements

II - 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.

II - 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.

II - 4.3.2.3 Risk Assessment

This capability will require CDM solutions to collect information about attributes in the MDR, MUR, MSR, and MIR to use with risk scores developed per C_Group-OR-1-2 (Section II – 1.6) using the FISMA and OU context of the information system.

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.

II - 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.

II - 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

II - 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 SCRM concepts are used to reduce the attack surface for network and infrastructure components in the Design, Development, and Deployment areas of the system component SDLC.

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

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

The DBS Development area focuses on developing and testing the information system to ensure that information system security and privacy needs are implemented effectively. This includes implementing secure coding practices, ensuring safeguards for sensitive information, and identifying and addressing security weaknesses and vulnerabilities. Secure coding practices include fail-safe coding, critical code review, and secure code re-use. Weaknesses and vulnerabilities in this area are identified using a variety of testing methods on both source and compiled code. The Development area of the SDLC incorporates configuration and version management to track and minimize the introduction of errors (weaknesses and vulnerabilities) into information systems. Weakness and vulnerability testing supports the ability to identify and remediate errors that are introduced during the development of information systems.

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

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

II - 4.4.1 DBS Operational Requirements

II - 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.

II - 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).

II - 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.[7]

II - 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.

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.

II - 4.4.2 DBS Functional Requirements

II - 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.

II - 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.

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

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

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

II - 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.[8]

II - 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

[8] 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).

- Attack surface mapping and analysis tools
- Hardening operating system tools
- Problem tracking tools
- Software signing tools

II - 5 Requirements to Manage "How Is Data Protected?"

Managing "How is data protected?" builds on the CDM capabilities provided by "What is on the network?", "Who is on the network?" and "What is happening on the network?".

"How is data protected?" focuses on the protection of sensitive (especially privacy) data,[9] which is covered by the following five capabilities:

1. Data Discovery/Classification (II - 5.2) describes techniques for the identification, discovery, and classification of data.
2. Data Protection (II – 5.3) describes data protection techniques.
3. Data Loss Prevention (II – 5.4) describes techniques to minimize the loss of data.
4. Data Breach/Spillage Mitigation (II – 5.5) describes techniques for response and recover activities due to data breach/spillage.
5. Information Rights Management (II – 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.

"How is data protected?" 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

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

- 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[10] as the source definition for "sensitive unclassified information" (i.e., sensitive data). This includes sensitive information subject to privacy protections (i.e., privacy data).

II - 5.1 Common Data Protection Requirements

Common data protection requirements describe data constructs applicable to the five subsequent data protection capabilities identified in Sections II-5.2 through II-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.

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

II - 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.

II - 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.

II - 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.[11]

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.

II - 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

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

II - 5.3 Data Protection (DATA_PROT) Requirements

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

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

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

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

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

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

II - 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.

II - 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),[12] or adaptive access control/risk-based access control.

II - 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

II - 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:

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

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

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

II - 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.

II - 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.

II - 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

II - 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.

II - 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:
    - Identify logical or physical compromise of information, system(s), and/or component(s)
    - Identify other information sources, systems, and/or components that may have also been compromised
    - Isolate the compromised information, system(s), and/or component(s)
    - Restore/recover operations through mitigation and/or remediation
    - Provide notification to data owners about the type of data spillage and impact
    - 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:

  - Organizational stakeholders (e.g., response staff, legal counsel, organizational management)
  - Mandatory response and recovery training for staff involved in response and recovery
  - 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

II - 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 work flow 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.

II - 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.

II - 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 boarders 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.

II - 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 (IAM), to include attributes (e.g., Active Directory)

h. Multimedia collaboration and information sharing platforms supporting internal and external users

II - 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

III - References

1) Continuous Diagnostics and Mitigation (CDM) System Architecture: Architecture Principles Document, Version 0.5, August 31, 2016

2) Federal Information Security Modernization Act of 2014, Public Law 113-283

3) Cybersecurity Enhancement Act of 2014, Public Law 113–274

4) The Privacy Act of 1974 (As Amended), Public Law 93-579

5) Code of Federal Regulations (CFR) Part 2002, Executive Order 13556 "Controlled Unclassified Information"

6) NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

7) NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

8) NIST FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

9) NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

10) NIST SP 800-63 Revision 3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3

11) NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

12) NIST SP 800-126 Revision 3, *The Technical Specification for the Security Content Automation Protocol (SCAP), SCAP Version 1.3*, February 2018, https://doi.org/10.6028/NIST.SP.800-126r3

13) NIST SP 800-162 *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, January 2014, http://dx.doi.org/10.6028/NIST.SP.800-162

14) NIST SP 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organization*, December 2016, https://doi.org/10.6028/NIST.SP.800-171r1.

15) NIST Interagency Report (NISTIR) 7298 Revision 2, *Glossary of Key Information Security Terms*, May 2013, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

16) NISTIR 7502 *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities,* December 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7502.pdf

17) NISTIR 8112 (Draft), *Attribute Metadata*, January 2018, http://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8112.pdf

18) NIST, *Survey on Access Control Models* (Draft), August 2009, https://csrc.nist.gov/csrc/media/events/privilege-management-workshop/documents/pvm-model-survey-aug26-2009.pdf

19) NIST, *DATA INTEGRITY Recovering from a destructive malware attack*, May 2016, (https://nccoe.nist.gov/sites/default/files/library/project-descriptions/data-integrity-project-description-final.pdf)

20) NIST, *Software Defined Virtual Networks* (https://www.nist.gov/programs-projects/software-defined-virtual-networks)

21) OMB M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

22) OMB M-17-09, *Management of Federal High Value Assets*, December 9, 2016

23) Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf

24) Federal Rules of Evidence, http://www.uscourts.gov/file/rules-evidence

25) National Vulnerability Database, (NVD) https://nvd.nist.gov/

26) Common Platform Enumeration, (CPE) https://nvd.nist.gov/products/cpe

27) Common Configuration Enumeration, (CCE) https://nvd.nist.gov/config/cce/index

28) CVE®, https://nvd.nist.gov/vuln/search

29) Common Weakness Enumeration (CWE), https://nvd.nist.gov/vuln/categories

30) Federated Identity, Credential, and Access Management (FICAM), https://www.idmanagement.gov

31) Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (X.509 ITU-T), http://www.itu.int/rec/T-REC-X.509/en

IV - Appendix A: Acronyms, Terms, and Definitions

Sources for the definitions include NIST SP 800-53r4, NISP SP 800-63r3, NISTIR 7298r2, NISTIR 8112 (draft), and NIST Survey on Access Control Models.

Table 1: Acronyms, Terms and Definitions

Acronym	Term	Definition
ACL	Access Control List	An ACL is a list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.
	Adaptive Access Control	Adaptive Access Control combines the subject credentials and contextual information to determine the risk of granting the requested action be performed on an object and may add dynamic elements to ABAC through functions like additional authentication steps (e.g., static/dynamic knowledge-based authentication, one-time passwords, cryptographic authenticator).
	Application Encryption	Application encryption is encryption of sensitive files or specified columns in a database using an application programing interface (API).
API	Application Program Interface	An API is a set of subroutine definitions (interfaces) and tools for building application software. They enable programs to access a common suite of capabilities through a defined connection.
	Attribute	An attribute is a quality or characteristic ascribed to someone or something. For example, an attribute may be a set of labels, values, and hierarchies that describe a characteristic or dimension of a CDM object.
ABAC	Attribute-based Access Control	ABAC is access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

Acronym	Term	Definition
	Attribute Values	Attribute values are data describing an asserted value for an associated attribute. For example, an attribute value may be a list of possible value assignments or types for an attribute that may be independent of format. For the attribute “birthday,” the value could be “12/1/1980” or “December 1, 1980.”
BEHAVE	Manage Security-Related Behavior	The CDM BEHAVE capability ensures that authorized users with or without special security responsibilities exhibit the appropriate behavior for their role.
	Behavior Deficiency	A behavior deficiency is a deficiency in compliancy. For example, an expired training cert is a behavior deficiency – the user failed to renew the cert as required.
	Behavior Incident	A behavior incident is an incident detected from an observed change from the normal behavior of a system, environment, process, workflow, or person (components).
BOUND	Boundary Protection	The CDM BOUND capability provides boundary protection for the interior of the network from all interconnections to other external networks.
CA	Certificate Authority	A Certificate Authority that acts as a trusted third party to facilitate a secure communication between users over a PKI framework.
CD	Compact Disk	A CD is a piece of storage media for digital data. The medium is used to store digital data and is widely used for software and other computer files.
CDM	Continuous Diagnostics and Mitigation	The CDM program provides Federal Departments and Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and allocate cybersecurity resources more efficiently.

Acronym	Term	Definition
	CDM Dashboard	The CDM dashboard is the tool that aggregates and displays CDM information at the Agency or Federal level. The dashboard provides consistent, timely, targeted, and prioritized information to security decision makers from cross-Agency and Federal-level managers to systems administrators to identify and support fixing the worst problems first.
CMaaS	Continuous Monitoring as a Service	CMaaS is the collection of elements that are not in the scope of the CDM Dashboard.
CRED	Credentials and Authentication Management	The CRED capability ensures that only proper credentials are authenticated to systems, services, and facilities.
	Cryptographic Anchoring	Cryptographic anchoring is encryption using a Hardware Security Module (HSM) solution that imposes data encryption/decryption within an Agency's infrastructure and restricts the rate of decryption actions to limit the rate of data exfiltration.
CSF	Cybersecurity Framework	The NIST Cybersecurity Framework (CSF) is a set of industry standards and best practices to help organizations manage cybersecurity risks. The Framework was created through collaboration between government and the private sector. It uses a common language to address and manage cybersecurity risk in a cost-effective manner based on business needs while minimizing imposition of additional regulatory requirements on businesses. The CSF is required under OMB Memorandum 16-03, "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements." It calls out the Federal adoption of the NIST CSF for improving critical infrastructure cybersecurity.
CSM	Configuration Settings Management	CSM ensures that authorized security configuration benchmarks exist and contain acceptable value(s) for each relevant configurable setting for each IT asset type.

Acronym	Term	Definition
CUI	Controlled Unclassified Information	CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
CVE®	Common Vulnerabilities and Exposures	CVE® is list of entries, each containing a CVE identifier, a description, and references for publicly known cybersecurity vulnerabilities.
CWE	Common Weakness Enumeration	The CWE specification provides a common language for discussing, finding, and dealing with the causes of software security vulnerabilities found in code, design, or system architecture.
	Data Element	A data element is a piece of information about CDM objects, their attributes, and/or associated policy to support the identification of defects.
DATA	Data Protection	The CDM DATA capability provides data protection functions to ensure the confidentiality and integrity of data and to respond to data leak/loss.
DATA_DISCOV	Data Discovery/Classification	The CDM DATA capability that supports data protection functions through data identification, data classification, and data tagging.
DATA_DLP	Data Loss Prevention Protection	The CDM DATA capability that provides data protection functions through data loss prevention capabilities, to include data protection policy management and data protection security orchestration.
DATA_IRM	Information Rights Management Data Protection	The CDM DATA capability that provides data protection functions through information rights management capabilities using fine-grained access control to encrypted data.
DATA_PROT	Data Protection	The CDM DATA capability that provides data protection functions through cryptography, masking/obfuscation, or access control.
DATA_SPIL	Data Breach/Spillage Response	The CDM DATA capability that provides data breach/spillage response actions.

Acronym	Term	Definition
DBS	Design and Build in Security	DBS describes preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment.
DEFEND	Dynamically Evolving Federal Enterprise Network Defense	DEFEND is a solicitation program under CDM that ensures requirements specified as part of acquisition are consistent with the overarching goal of enabling U.S. Government entities to assess and improve the security posture of an Agency's information systems.
	De-identification/ Pseudonymity	De-identification/Pseudonymity replaces privacy-related sensitive data with generic (e.g., token) information that maintains the anonymity of the source information.
DAC	Discretionary Access Control	DAC implements an access matrix model to determine which subjects (users/applications) are permitted to perform actions (read, write, modify, change permissions, execute) on which objects/resources (files, directories).
DHS	Department of Homeland Security	The DHS is a Federal Agency whose missions include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience.
DLP	Data Loss Prevention	DLP are processes that provide consistent protection to block exfiltration across the organization for processing, storing, and transmitting data and use capabilities and functions.
DRM	Digital Rights Management	DRM is a group of access control technologies that extends across various digital media.
DVD	Digital Video Disc	A DVD is digital optical disc storage media invented in 1995. The medium is used to store digital data and is widely used for software and other computer files.
ETL	Extraction-Transformation-Load	ETL are "three" processes performed when moving raw data from the source to a data repository such as a warehouse, data mart, or relational database.

Acronym	Term	Definition
FIPS	Federal Information Processing Standards	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the NIST for Federal computer systems. These standards and guidelines are issued by NIST as FIPS for use Government-wide.
FISMA	Federal Information Security Management Act 2002 Federal Information Security Modernization Act 2014	FISMA is the U.S. legislation defining a comprehensive framework to protect Government information, operations, and assets against natural or man-made threats. FISMA 2002 (Public Law 107-347) was signed into law part as of the Electronic Government Act of 2002. FISMA 2002 requires Federal Agencies to develop, document, and implement an Agency-wide program to provide information security for the information and information systems supporting operations and assets within the Agency. In addition to changing Management to Modernization, FISMA 2014 (Public Law 113-283) updates the Federal Government's cybersecurity practices by: • Codifying (DHS authority to administer the implementation of information security policies for non-national security Federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems; • Amending and clarifying OMB oversight authority over Agency information security practices; • Driving the revision of OMB A-130 to "eliminate inefficient and wasteful reporting."
	File Encryption	File encryption is the encryption of individual files based either on system policies (enforced) or at the user's discretion (ad hoc).
	Format Preserving Encryption	Format Preserving Encryption replaces sensitive data with an encrypted version that maintains the format of the source data (i.e., ensures the encrypted form of the sensitive data conforms to the rules [e.g., length, character set] for the sensitive data).

Acronym	Term	Definition
	Full Disk Encryption	Full disk encryption is the automatic encryption of all data stored on the device by the device, operating system, or a third-party application. • A self-encrypting drive (SED) encrypts the entire hard disk (including the operating system) using hardware. • Native full storage encryption (FSE) encrypts the entire disk (including the operating system) except for files needed to boot the system. Native FSE is included as part of the operating system for the device. • Third-party FSE operates like native FSE, but is independent of the operating system. Third-party FSE modifies the boot loader to support encrypting the hard drive.
HWAM	Hardware Asset Management	The HWAM Function is to discover unauthorized or unmanaged hardware on a network.
IAM	Identity and Access Management	IAM provides identity proofing and authentication aspects under identity management. IAM supports the use, maintenance, and protection of sensitive information such as PII collected from users.
IRM	Information Rights Management	IRM controls access to enterprise information (e.g., documents, files) under DRM.
IT	Information Technology	IT is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency.
MAC	Mandatory Access Control	MAC is an access control feature controlled at the operating system level, where the operating system kernel examines the attributes of a subject that is attempting to access an object.
MDR	Master Device Record	MDR is a set of attributes or assertions about a user, with the device as the primary key.
MIR	Master Incident Record	MIR represents activities associated with security controls that require an action when an event occurs; deals with “What is happening on the network?”

Acronym	Term	Definition
MNGEVT	Manage Events	MNGEVT describes preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through analysis of data.
MSR	Master System Record	The MSR is a set of attributes or assertions about a user, with the system as the primary key.
MUR	Master User Record	The MUR is a set of attributes or assertions about a user, with the user as the primary key.
NARA	National Archives and Records Administration	NARA is the Federal Agency tasked with maintaining Federal records and archives.
NIST	National Institute of Standards and Technology	NIST is the Federal Agency that works with industry to develop and apply technology, measurements, and standards.
NTP	Network Time Protocol	NTP is a networking protocol for clock synchronization between computers and devices. It is designed to provide synchronization over packet-switched, variable-latency data networks. NTP version 3 is specified in the Request for Comment (RFC) 1305 standard.
	Numeric Variance	Numeric variance is a process in which the numeric values that are stored within a development database can be changed, within a defined range, so as not to reflect their actual values within the production database. Numeric variance replaces sensitive data with a random value within a specified range of the source data.
OMB	Office of Management and Budget	OMB is the business division of the Executive Office of the President of the United States that administers the United States Federal budget and oversees the performance of Federal Agencies.
	Ongoing Assessment	Ongoing assessment is the continuous evaluation of the effectiveness of security control implementations. Under CDM, ongoing assessment is the continuous process of comparing security-related and privacy related container and object attributes between the actual state and the desired state.

Acronym	Term	Definition
OMI	Operate, Monitor and Improve	OMI describes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).
OU	Organizational Unit	An OU is the Government Department or Agency, or an entity within the Agency, responsible for the information system.
PACS	Physical Access Control System	PACS is an automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
PDP	Policy Decision Point	PDP is a repository for policies that are distributed to enforcement points; mediates or de-conflicts DPs per MPs in some implementations.
PEP	Policy Enforcement Point	PEP is a service that resides on and directly interacts with network objects (e.g., servers, asset scanners, firewalls), which exchanges policy-related messages with the Policy Decision Point. The PEP enforces organizational policy via the configuration applied to the object.
PRIV	Managing Account Access Capability	PRIV is a CDM capability to provide the Agency with the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.
	Privacy Data	Privacy data includes any data subject to the Privacy Act of 1974, as amended. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI), among others.
	Redaction/Suppression	Redaction/suppression removes or encrypts sensitive data to protect the sensitive data. This differs from other masking methods that attempt to maintain realism in the masked data set.
	Risk-based Access Control	See Adaptive Access Control
RMF	Risk Management Framework	The RMF is a structured approach used to oversee and manage risk for an enterprise.

Acronym	Term	Definition
RBAC	Role-based Access Control	RBAC manages access to objects in a manner that closely resembles the organizational structure, using one or more roles assigned to subjects.
SCRM	Supply Chain Risk Management	SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/operational technology (OT) product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction), as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.
SDLC	System Development Life Cycle	SDLC is the process of planning, creating, testing, and deploying an information system. The SDLC concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.
	Shuffling	Shuffling replaces sensitive data with realistic masked data, similar to substitution, using the sensitive data as the source for masked data (vice an external data set). Data within a column is shuffled between records to perform the masking.
SIEM	Security Information and Event Management	A SIEM is an application providing the ability to gather security data from information system components and present that data as actionable information via common interface.
SP	Special Publication	NIST Special Publications include SP 800 subseries (computer security) and selected SP publications directly relevant to computer/ cyber/information security and privacy.
	Storage Container Encryption	Storage Container Encryption is encryption at the filesystem level for data partition and device volume.
	Substitution	Substitution replaces sensitive data with substitute data that appears to be real data using external files and/or databases with a mapping (to support consistency in substitution).
SWAM	Software Asset Management	The SWAM Function is to discover unauthorized or unmanaged software on a network.

Acronym	Term	Definition
TFA	Tool Functional Area	DHS is implementing the CDM program, made up of 15 BPA TFAs, that addresses “what is on the network,” “who is on the network,” and “what is happening on the network.”
	Tokenization	Tokenization replaces sensitive data with a tokenized version designed to be reversible (i.e., the sensitive data can be derived from the tokenized data), unlike other data masking techniques. • Vault-based tokenization – a random number generator is used to create a token via an asymmetric process (i.e., one-way) and maintain a vault that contains the mapping from the sensitive data to the tokenized data. • Vaultless tokenization – a process and secret key are used to derive a token for the substitution so that a vault (or mapping table) is not required.
TRUST	Manage Trust in People Granted Access Capability	This CDM capability assesses the inherent risk to an Agency from insider attacks for the purposes of granting trust to users and authorizing each user for certain attributes.
UEBA	User and Entity Behavior Analytics	UEBA is a process that takes note of the normal conduct of users and processes (i.e., defines normal behavior). UEBA can then be used to detect anomalous behavior (i.e., instances when there are deviations from the “normal” patterns).
VUL	Vulnerability Management	The VUL Function is to discover and support remediation of vulnerabilities in IT assets on a network as defined in NIST SP 800-53 controls.

V - Appendix B: NIST Cybersecurity Framework Crosswalk

This section presents a high-level crosswalk between the *Continuous Diagnostics and Mitigation (CDM) Technical Capabilities, Volume Two Requirements Catalog* and the *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. A more detailed analysis is available within the CDM Companion I-2.

Table 2: CDM Volume Two Functional Requirements to NIST CSF Crosswalk

Section	Section Title	Category and Function
II	All CDM Capabilities	The following three CSF Categories apply to all CDM capabilities: • Governance (ID.GV) under IDENTIFY • Security Continuous Monitoring (DE.CM) under DETECT • Anomalies and Events (DE.AE) under DETECT
II-2.1.2	HWAM Functional Requirements	• Asset Management (ID.AM) under IDENTIFY • Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT
II-2.2.2	SWAM Functional Requirements	• Asset Management (ID.AM) under IDENTIFY • Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT
II-2.3.2	CSM Functional Requirements	• Risk Assessment (ID.RA) under IDENTIFY • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT • Maintenance (PR.MA) under PROTECT
II-2.4.2	VUL Functional Requirements	• Risk Assessment (ID.RA) under IDENTIFY • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT • Maintenance (PR.MA) under PROTECT
II-3.1.2	TRUST Functional Requirements	• Risk Assessment (ID.RA) under IDENTIFY • Identity Management, Authentication and Access Control (PR.AC) under PROTECT

Section	Section Title	Category and Function
II-3.2.2	BEHAVE Functional Requirements	• Awareness and Training (PR.AT) under PROTECT • Communications (RS.CO) under RESPOND
II-3.3.2	CRED Functional Requirements	• Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Protective Technology (PR.PT) under PROTECT
II-3.4.1	PRIV Functional Requirements	• Asset Management (ID.AM) under IDENTIFY • Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Protective Technology (PR.PT) under PROTECT • Communications (RS.CO) under RESPOND
II-4.1.1.2	BOUND-F Functional Requirements	• Asset Management (ID.AM) under IDENTIFY • Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT • Protective Technology (PR.PT) under PROTECT • Detection Processes (DE.DP) under DETECT
II-4.1.2.2	BOUND-E Functional Requirements	• Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Data Security (PR.DS) under PROTECT • Protective Technology (PR.PT) under PROTECT
II-4.1.3.2	BOUND-P Functional Requirements	• Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Detection Processes (DE.DP) under DETECT
II - 4.2.2.1	Incident Response Monitoring	• Asset Management (ID.AM) under IDENTIFY • Detection Processes (DE.DP) under DETECT • Analysis (RS.AN) under RESPOND
II - 4.2.2.2	Privacy Monitoring	• Data Security (PR.DS) under PROTECT
II - 4.2.2.3	Contingency Planning Monitoring	• Business Environment (ID.BE) under IDENTIFY • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT
II - 4.2.2.4	Audit Data Collection	• Detection Processes (DE.DP) under DETECT • Analysis (RS.AN) under RESPOND
II - 4.2.2.5	Ongoing Assessment Monitoring	• Detection Processes (DE.DP) under DETECT
II - 4.3.2.1	Ongoing Authorization	• Analysis (RS.AN) under RESPOND • Mitigation (RS.MI) under RESPOND

Section	Section Title	Category and Function
II - 4.3.2.2	System and Information Integrity	• Information Protection Processes and Procedures (PR.IP) under PROTECT • Maintenance (PR.MA) under PROTECT • Protective Technology (PR.PT) under PROTECT • Detection Processes (DE.DP) under DETECT • Analysis (RS.AN) under RESPOND • Mitigation (RS.MI) under RESPOND
II - 4.3.2.3	Risk Assessment	• Risk Assessment (ID.RA) under IDENTIFY • Risk Management (ID.RM) under IDENTIFY • Analysis (RS.AN) under RESPOND
II - 4.3.2.4	Security Assessment and Authorization	• Analysis (RS.AN) under RESPOND • Mitigation (RS.MI) under RESPOND • Improvements (RS.IM) under RESPOND • Recovery Planning (RC.RP) under RECOVER • Improvements (RS.IM) under RECOVER
II-4.4.2.1	DBS Design	• Risk Assessment (ID.RA) under IDENTIFY • Risk Management (ID.RM) under IDENTIFY
II-4.4.2.2	DBS Development	• Business Environment (ID.BE) under IDENTIFY • Risk Assessment (ID.RA) under IDENTIFY
II-4.4.2.3	DBS Deployment	• Risk Assessment (ID.RA) under IDENTIFY • Analysis (RS.AN) under RESPOND
II-5.2.2	DATA_DISCOV Functional Requirements	• Asset Management (ID.AM) under IDENTIFY
II-5.3.2	DATA_PROT Functional Requirements	• Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT • Protective Technology (PR.PT) under PROTECT
II-5.4.2	DATA_DLP Functional Requirements	• Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT • Protective Technology (PR.PT) under PROTECT • Response Planning (RS.RP) under RESPOND • Mitigation (RS.MI) under RESPOND • Recovery Planning (RC.RP) under RECOVER

Section	**Section Title**	**Category and Function**
II-5.5.2	DATA_SPIL Functional Requirements	• Response Planning (RS.RP) under RESPOND • Mitigation (RS.MI) under RESPOND • Recovery Planning (RC.RP) under RECOVER
II-5.6.2	DATA_IRM Functional Requirements	• Identity Management, Authentication and Access Control (PR.AC) under PROTECT • Data Security (PR.DS) under PROTECT • Information Protection Processes and Procedures (PR.IP) under PROTECT • Protective Technology (PR.PT) under PROTECT