

SIN 541519CDM Continuous Diagnostics and Mitigation (CDM) Tools

Additional SIN Description: The Continuous Diagnostics and Mitigation (CDM) Tools SIN supports the Department of Homeland Security (DHS) CDM Program. The hardware and software products and associated services under this SIN undergo a DHS product qualification process in order to be added to the CDM Approved Products List (APL). The full complement of SIN products and services includes tools, associated maintenance, and other related activities such as training. The CDM Program is organized by the following 5 CDM capabilities:

- 1. Asset Management:** Identifies the existence of hardware, software, configuration characteristics and known security vulnerabilities.
- 2. Identity and Access Management:** Identifies and determines the users or systems with access authorization, authenticated permissions and granted resource rights.
- 3. Network Security Management:** Prepares for events/incidents, gathers data from appropriate sources; and identifies incidents through analysis of data.
- 4. Data Protection Management:** Focuses on the protection of sensitive data (Especially privacy) covered by data discovery/classification, protection, loss prevention, breach/spillage mitigation and information rights management.
- 5. Future Capabilities:** Includes CDM cybersecurity tools and technology not in any other group.

The 5 capability groups represent the scope of the CDM program and reflect widely exercised functional and operational scenarios that CDM is interested in identifying, monitoring and addressing from a security perspective.

To provide a holistic security approach, these capabilities adhere to the National Institute of Science and Technology (NIST) Cybersecurity Framework security functions to identify, protect, detect, respond and recover. CDM also supports and can be used in the NIST Risk Management Framework (RMF) to achieve ongoing assessment and authorization.

As shown in Table 1, the CDM Tools SIN scope covers the 5 CDM Program Capabilities.

Table 1: SIN Scope to Capability mapping

CDM Capability Groups	Capabilities
1. Asset Management	<ul style="list-style-type: none"> ● Hardware Asset Management ● Software Asset Management ● Configuration Settings Management ● Vulnerability Management

2. Identity and Access Management	<ul style="list-style-type: none"> • Manage Trust in People Granted Access • Manage Security-Related Behavior • Manage Credential and Authentication • Manage Account/Access/Manage Privileges
3. Network Security Management	<ul style="list-style-type: none"> • Prepare for Contingencies and Incidents • Respond to Contingencies and Incidents • Design and Build in Requirements Policy and Planning • Design and Build in Quality • Manage Audit Information • Manage Operation Security • Manage Network Access Controls
4. Data Protection Management	<ul style="list-style-type: none"> • Data Discovery/Classification • Data Protection • Data Loss Prevention • Data Breach/Spillage Mitigation • Information Rights Management
5. Future Capabilities	Future innovations

1. Asset Management

Focus: The primary focus of Asset Management is to identify “What is on the network?”; that is, to identify the existence of hardware, software, configuration characteristics and known security vulnerabilities.

Manage hardware and software baseline system inventory is based on Hardware Asset Management (HWAM) and Software Asset Management (SWAM) requirements that requires the discovery and identification of devices to define a baseline of inventory hardware and software assets to establish the Agency’s span of control.

Hardware and software configurations are based on Configuration Settings Management (CSM) requirements to ensure that hardware and software (specifically the operating system and installed applications) assets are securely configured and hardened.

Manage vulnerabilities is based on Vulnerability Management (VUL) requirements to identify and manage vulnerabilities in software installed on network devices to minimize exploitation of known software weaknesses.

These CDM capabilities cover verification and validation for the existence of hardware infrastructure devices; the accurate identification of approved software components; verification and validation that hardware devices have the correct security configuration settings, and system platform is hardened to reduce the platform attack surface; and the identification and management of risks presented by known software weaknesses that are subject to exploitation.

These CDM capabilities support the Cybersecurity Framework functions of: identify, protect and detect.

2. Identity and Access Management

Focus: The primary focus of Identity and Access Management is to determine “Who is on the network?”; that is, identify and determine the users or systems with authorized access.

Manage People is based on PRIV, CRED, TRUST and BEHAVE requirements that require the management of users/accounts as an asset to assure the appropriate individual has the right access to the right resource.

This CDM capability covers the verification and validation of allowed user privileges, issuance and management of user owned credentials, appropriate user security behavior training, trustworthiness, authenticated permissions, and management of resource access rights granted to users.

These CDM capabilities support the Cybersecurity Framework functions of: identify, protect and detect.

3. Network Security Management

Due to the complexity to manage “What is happening on the network?”, this area is covered by four focus areas:

- a. Boundary Protection (BOUND)
- b. Manage Events (MNGEVT)
- c. Operate, Monitor and Improve (OMI)
- d. Design and Build in Security (DBS)

Boundary Protection

Focus: The primary focus of Boundary Protection is to determine “How is the boundary protected?”; that is, to determine the user/system actions and behavior at the physical/logical network boundaries and within the computing infrastructure.

“How is the boundary protected?” is based on BOUND requirements to defend physical and logical network boundaries and identify abnormal behavior (of networks and users) that may identify that an incident has occurred.

This CDM capability covers verification and validation of logical and physical network interfaces to reduce intrusive, malicious, and disruptive attacks; cryptographic mechanisms to ensure confidentiality and integrity of data on the network; and methods to identify security incidents.

These CDM capabilities support the Cybersecurity Framework functions of: identify, protect and detect.

Manage Events

Focus: Manage Events is responsible for preparing for events/incidents, gathering appropriate audit data from appropriate sources, identifying incidents through analysis of data, and performing ongoing assessment.

Manage Events is based on the MNGEVT requirements to prepare for incidents/events (through processes, policies, and procedures), gather appropriate audit/log data from appropriate sources, and identify events/incidents (network and user abnormal behavior) through the analysis of audit/log data.

Manage Events supports the runtime collection of attributes (actual state) and continuous monitoring of the policies related to attributes for Ongoing Assessment (actual state vs. desired state) to enhance current or apply new security and privacy controls and countermeasures. The results of the Ongoing Assessment will be used as inputs to OMI Ongoing Authorization risk assessment process to determine if the level of risk remains acceptable for a given information system to support continued authorization and operation.

Ongoing Assessment is the continuous process of comparing security related attributes between the Actual State and the Desired State. This comparison is performed by the CDM Policy Decision Point (PDP). The discrepancy between Actual State and Desired state impacts the security posture of the implementation of NIST SP 800-53 controls and countermeasures. The results of the Ongoing Assessment are used to evaluate the changes in risk posture associated with the discrepancy. Ideally, the Ongoing Assessment process is fully automated with the Desired State being encoded in the CDM PDP and the Actual State being measured using CDM sensors.

This CDM capability covers verification and validation of processes, policies, and procedures supporting cybersecurity preparation, audit and log data collection, security analysis of audit/log data, incident reporting to provide forensic evidence of malicious or suspicious behavior, and ongoing assessment.

To provide a holistic security approach, this capability adheres to the Cybersecurity Framework security functions to identify, protect, detect, respond and recover CDM also supports and can be used in the NIST Risk Management Framework (RMF) to achieve ongoing assessment and authorization.

Operate, Monitor and Improve

Focus: Operate, Monitor and Improve is responsible for audit data aggregation, correlation, and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).

Operate, Monitor and Improve is based on OMI requirements for audit data aggregation, correlation and analysis, incident prioritization and response, and post incident activities (e.g., information sharing).

Ongoing Authorization is the continuous evaluation of the change in risk level related to changes in security policies concerning static object attributes (i.e., actual state and desired state) for threat behaviors that impact the security posture. This impact to security is measured by capturing changes in existing safeguards (e.g., NIST SP 800-53 controls and countermeasures) and identification of new component weaknesses and vulnerabilities.

This CDM capability covers verification and validation of processes/procedures to aggregate, correlate, and analyze audit/log data, to prioritize incidents and associated response actions, to quickly mitigate the impact of an incidents, to take appropriate remediation actions to eliminate the impact (restore normal operations) of the same incident, to support information sharing and collaboration (both internal and external) to minimize or prevent impact of future incidents, and ongoing authorization.

To provide a holistic security approach, this capability adheres to the Cybersecurity Framework security functions to identify, protect, detect, respond and recover. CDM also supports and can be used in the NIST Risk Management Framework (RMF) to achieve ongoing assessment and authorization.

Design and Build in Security

Focus: Design and Build in Security is responsible for preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment. The Design and Build in Security process is focused on identifying, controlling and removing weaknesses/vulnerabilities from the software/system. Exploitable vulnerabilities may include software/system design, coding errors, software/system designs that leave a large and complex attack surface that cannot be defended, and weaknesses that can only be exploited during system/software execution.

Design and Build in Security is based on the DBS requirements that extend the focus of Software Asset Management and Vulnerability Management to achieve a level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle and that the software functions in the intended manner.

The U.S. government and critical infrastructure sectors are increasingly dependent on commercial products and systems, which present significant benefits including low cost, interoperability, rapid innovation, a variety of product features, and choice among competing vendors. However, with some of these benefits there is an increase in the risk of a threat event

which can directly or indirectly affect the supply chain, which often go undetected, and may result in risks to the acquirer. The purpose of Supply Chain Risk Management (SCRM) is to enable the provisioning of the least vulnerable solutions to agencies, through a robust assessment of supply chain risks, communication about those risks to the agencies, and appropriate response and monitoring of those risks throughout the entire system lifespan.

This CDM capability covers verification and validation of processes/procedures to prevent and detect software vulnerabilities, to determine the provenance of system components, and to measure software assurance for built and acquired software components.

To provide a holistic security approach, this capability adheres to the Cybersecurity Framework security functions to identify, protect, detect, respond and recover.

4. Data Protection Management

Focus: Managing “Data Protection builds on the CDM capabilities provided by Asset Management, Identity and Access Management, Boundary Protection, and Network Security Management. Data Protection Management focuses on the protection of sensitive (especially privacy) data, which is covered by the following five capabilities Data Discovery Classification, Data Protection, Data Loss Prevention, Data Breach/Spillage Mitigation and Information Rights Management.

Sensitive (especially privacy) data requires both security and data protections to ensure the confidentiality, integrity, and availability of data assets, while at rest, in use and in transit. These data protections are focused on the use the National Archives and Records Administration’s (NARA) Controlled Unclassified Information (CUI) registry¹ as the source definition for “sensitive unclassified information” (i.e., sensitive data).

Data Protection Management covers the establishment of policies, the management of data protection processes and the automation for IDENTIFY via classification and discovery.

5. Future Capabilities

Focus: Innovative capabilities to cybersecurity not currently encompassed by the other capability areas.

¹ See <https://www.archives.gov/cui/registry/category-list>.