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) Cybersecurity and Infrastructure Security Agency (CISA) 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 five (5) CDM capability areas:

1. **Asset Management**
2. **Identity and Access Management (IDAM)**
3. **Network Security Management (NSM)**
4. **Data Protection Management (DPM)**
5. **Future Capabilities**

Note: *Please visit the Continuous Diagnostics & Mitigation (CDM) Program webpage at "gsa.gov/cdm", for more information on the CDM APL submission process.*

The five (5) capability areas 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 Standards 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 five (5) CDM Program Capabilities.

Table 1: SIN Scope to Capability Mapping

CDM Capability Areas	Functional Requirements
1. Asset Management	● Hardware Asset Management (HWAM) ● Software Asset Management (SWAM) ● Configuration Settings Management (CSM) ● Vulnerability Management (VUL) ● Enterprise Mobility Management (EMM)
2. Identity and Access Management (IDAM)	● Trust determination for people granted access (TRUST) ● Security-related behavioral training (BEHAVE) ● Credentials and authentication (CRED) ● Management and control of account and access privileges (PRIV)

3. Network Security Management (NSM)	● Manage BOUND, or "How is the network protected?" ● Manage Events (MNGEVT) Requirements ● Operate, Monitor, and Improve (OMI) Requirements ● Design and Build in Security (DBS) Requirements ● Manage Audit Information ● Manage Operation Security
4. Data Protection Management (DPM)	● Common Data Protection Requirements ● Data Discovery/Classification (DATA_DISCOV) Requirements ● Data Protection (DATA_PROT) Requirements ● Data Loss Prevention (DATA_DLP) Requirements ● Information Rights Management (DATA_IRM) Requirements
5. Future Capabilities	Future innovations

1. Asset Management Capability Area

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

These functions are briefly summarized below, and the requirements are separately specified in the "CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM, Technical Capabilities, Volume Two: Requirements Catalog 2020", HWAM, SWAM, CSM, VUL, and EMM sections.

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

2. IDAM Capability Area

This capability area addresses "Who is on the Network" to strengthen management of users and accounts on Agency networks. The IDAM capabilities focus on identifying Agency users, ensuring that they have been properly identified, vetted, trained, and authenticated.
These functions are briefly summarized below, and the requirements are separately specified in the "CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM, Technical Capabilities, Volume Two: Requirements Catalog 2020", TRUST, BEHAVE, CRED, and PRIV sections.
The four component capabilities are:

1. Trust determination for people granted access (TRUST). TRUST functional requirements relate to the identity origination and background investigations performed on the user.

2. Security-related behavioral training (BEHAVE). BEHAVE functional requirements relate to the training and certifications required and completed.
3. Credentials and authentication (CRED). CRED functional requirements track the users' credentials and the systems and accounts assigned to which the user.
4. Management and control of account and access privileges (PRIV). PRIV functional requirements identify systems to which users have access and their privileges on those systems.

3. NSM Capability Area

This capability area builds on the CDM capabilities provided by Asset Management and Identity and Access Management. The NSM capabilities include network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. NSM is broken into four capabilities.

These capabilities are briefly summarized below, and the detailed requirements are separately specified in the "CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM, Technical Capabilities, Volume Two: Requirements Catalog 2020", BOUND, MNGEVT, OMI, and DBS sections. The four component capabilities are:

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

4. DPM Capability Area

This capability area focuses on "How is data protected?" and builds on the CDM capabilities provided by Asset Management, Identity and Access Management, and Network Security Management.

DPM is broken into five (5) capabilities. These capabilities are briefly summarized below, and the detailed requirements are separately specified in the "CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM, Technical Capabilities, Volume Two: Requirements Catalog 2020", DPM section. The five capabilities are:

1. Data Discovery/Classification describes techniques for the identification, discovery, and classification of data.
2. Data Protection describes data protection techniques.
3. Data Loss Prevention describes techniques to minimize the loss of data.
4. Data Breach/Spillage Mitigation describes techniques for response and recover activities due to data breach/spillage.
5. Information Rights Management describes data protection functions specific to information rights management.

5. Future Capabilities

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