Continuous Diagnostics and Mitigation (CDM) Tools support 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 CDM subcategories includes tools, associated maintenance, and other related activities such as training. The SIN is organized by CDM capabilities into the following 5 subcategories:

Sub-Categories: *Vendors’ tools will be placed within the following subcategories.*

1. **Manage “What is on the network?”**: Identifies the existence of hardware, software, configuration characteristics and known security vulnerabilities.
2. **Manage “Who is on the network?”**: Identifies and determines the users or systems with access authorization, authenticated permissions and granted resource rights.
3. **Manage “How is the network protected?”**: Determines the user/system actions and behavior at the network boundaries and within the computing infrastructure.
4. **Manage “What is happening on the network?”**: Prepares for events/incidents, gathers data from appropriate sources; and identifies incidents through analysis of data.
5. **Emerging Tools and Technology**: Includes CDM cybersecurity tools and technology not in any other subcategory.

The 5 subcategories 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 5 CDM Tools SIN subcategories cover the previous 15 CDM Blanket Purchase Agreement (BPA) Tool Functional Areas (TFAs) and allow for future innovation.

Table 1: SIN to TFA mapping

<table>
<thead>
<tr>
<th>5 SIN Subcategories</th>
<th>15 CDM BPA TFAs</th>
</tr>
</thead>
</table>
| 1. Manage “What is on the network?” | ● TFA 1 – Hardware Asset Management  
● TFA 2 – Software Asset Management  
● TFA 3 – Configuration Settings Management  
● TFA 4 – Vulnerability Management |
| 2. Manage “Who is on the network?” | ● TFA 6 – Manage Trust in People Granted Access  
● TFA 7 – Manage Security-Related Behavior  
● TFA 8 – Manage Credential and Authentication  
● TFA 9 – Manage Account/Access/Manage Privileges |
| 3. Manage “How is the network protected?” for BOUND | ● TFA 5 – Manage Network Access Controls |
| 4. Manage “What is happening on the network?” for MNGEVT | ● TFA 10 – Prepare for Contingencies and Incidents  
● TFA 11 – Respond to Contingencies and Incidents  
● Ongoing Assessment |
| 4. Manage “What is happening on the network?” for DBS | ● TFA 12 – Design and Build in Requirements Policy and Planning  
● TFA 13 – Design and Build in Quality  
● Supply Chain Risk Management |
| 4. Manage “What is happening on the network?” for OMI | ● TFA 14 – Manage Audit Information  
● TFA 15 – Manage Operation Security  
● Ongoing Authorization |
5. Emerging Tools and Technology

Future innovations

1. Manage “What is on the network?”

**Focus:** The primary focus of Manage Assets 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 Phase 1 Hardware Asset Management (HWAM) and Software Asset Management (SWAM) requirements that discover and identify 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 Phase 1 Configuration Settings Management (CSM) requirements to ensure that hardware and software assets (specifically the operating system and installed applications) are securely configured and hardened.

Manage vulnerabilities is based on Phase 1 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; hardening of the system platform 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. Manage “Who is on the network?”

**Focus:** The primary focus of Manage People 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 Phase 2 PRIV, CRED, TRUST and BEHAVE requirements that require the management of users/accounts as an asset to ensure 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. Manage “How is the network protected?”

Focus: The primary focus of Manage Network 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 network protected?” is based on Phase 3 BOUND requirements to defend physical and logical network boundaries and identify abnormal behavior (of networks and users) that may identify when 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 the 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.

4. Manage “What is happening on the network?”

Due to the complexity to manage “What is happening on the network?”, this area is covered by three focus areas:
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 Phase 3 MNGEVT requirements to prepare for incidents/events (through processes, policies, and procedures), gather appropriate audit/log data from appropriate sources, and identify events/incidents (abnormal network and user 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 for OMI Ongoing Authorization risk assessment processes 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).

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 incident; to take appropriate remediation actions to eliminate the impact (i.e., restore normal operations) of the same incident; to support information sharing and collaboration (both internally and externally); to minimize or prevent the 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 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 Phase 3 DBS requirements that extend the focus of Phase 1 Software Asset Management and Vulnerability Management to achieve a level of confidence that software is free from vulnerabilities, either intentionally designed in 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-in 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.

5. Emerging Tools and Technology

Focus: Emerging Tools and Technology will feature innovative capabilities in cybersecurity not currently encompassed by the other capability areas.