IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM
OVERVIEW

DEFEND TODAY,
SECURE TOMORROW

The Cybersecurity and Infrastructure Security Agency (CISA) Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures by delivering better visibility and awareness of their networks and defending against cyber adversaries. The CDM Program ultimately reduces the threat surface and improves federal cybersecurity response through four capability areas: Asset Management, Identity and Access Management, Network Security Management, and Data Protection Management.

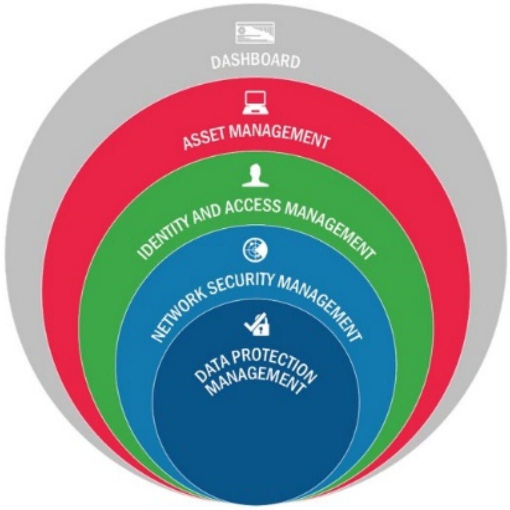
PROGRAM OBJECTIVES

The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture. Program objectives are to:

- **Reduce** agency threat surface
- **Increase** visibility into the federal cybersecurity posture
- **Improve** federal cybersecurity response capabilities
- **Streamline** Federal Information Security Modernization Act (FISMA) reporting

CDM CAPABILITIES

The CDM Program delivers capabilities in five key program areas (see figure).


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

CDM Program Capability Areas

- **Agency and Federal Dashboards:** Receives, aggregates, and displays information from CDM tools at the agency and federal levels.
- **Asset Management** – Manages hardware assets (HWAM), software assets (SWAM), security management configuration settings (CSM), and software vulnerabilities (VUL).
- **Identity and Access Management** – Manages account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related training (BEHAVE).
- **Network Security Management** – Manages network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. This includes management of events (MNGEVT); operate, monitor, and improve (OMI); design and build-in security (DBS); boundary protection (BOUND); supply chain risk management (SCRM); and ongoing authorization.
- **Data Protection Management** – Manages the protection of data through the capabilities: data discovery/classification (DISC), data protection (PROT), data loss prevention (DLP), data breach/spillage mitigation (MIT), and information rights management (IRM).

AGENCY AND FEDERAL DASHBOARDS

The CDM Program has deployed agency-level dashboards to 23 Chief Financial Officers (CFO) Act federal civilian agencies. The dashboards provide a window into the security posture of agency computers, servers, and other Internet-connected devices. The Agency Dashboard is a data visualization tool that produces customized reports, alerting information technology (IT) managers to the most critical cybersecurity risks. In parallel to the deployment of agency-level dashboards, CDM has established the Federal Dashboard. It is a tool which consolidates summary information from each agency-level dashboard to form a picture of cybersecurity health across all civilian agencies. This tactical summary data (e.g., critical patch status) will be used to inform strategic decision making regarding systemic cybersecurity risks across the Federal Government.

SHARED SERVICES

The CDM Shared Services Platform provides non-CFO Act agencies with access to CDM capabilities, leveraging a cost model and approach that is tailored to small and micro-agency resource constraints (e.g., funds and personnel). The data collected at the agency level is individual agency dashboards in a shared services environment. Summary data from the Agency Dashboards are reported to the CDM Federal Dashboard.

The platform extends current capabilities of the existing CDM Program into a delivery model that adheres to the core principles of a shared service. CDM shared services directly supports the Office of Management Budget Chief Information Officer's Federal Cloud Computing Strategy ("Cloud Smart") and the Federal Information Technology Shared Services Strategy ("Shared-First"), while also meeting the security objectives of the CDM Program.

The CDM Shared Services Platform 2.0 began providing services to 36 Agencies in June 2021. By the end of Fiscal Year 2022, it is anticipated that more than 50 agencies will be participating in this shared services model. CDM Shares Services Platform 2.0 boasts a service catalog of various tools that propels agencies to get CDM capabilities and use the dashboards to meet various data calls such as FISMA, Binding Operational Directives (BODs), and emorandum taskers.

ACQUISITION STRATEGY

The CDM acquisition strategy provides products and services to federal civilian agencies to meet CDM Program objectives. The strategy consists of the following components:

- **CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND)**
  CDM DEFEND is a series of task orders offering an all-encompassing approach for addressing CDM Program requirements. Each DEFEND task order is executed by an industry partner that is responsible for installing and deploying CDM capabilities at federal civilian agencies. DEFEND offers a wide array of benefits, such as providing flexibility to purchase new tools as they are developed and allowing agencies to shorten acquisition timelines by reducing the frequency of recompetes.

- **CDM Approved Products List (APL)**
  The CDM Program's APL is the authoritative catalog for approved products that meet CDM technical requirements. Software and hardware manufacturers and resellers can submit products for consideration monthly. CISA reviews each submission against established CDM Program criteria to validate the vendor's claim that each product meets the requirements for the capability category for which it was submitted. The CDM APL includes tools, associated maintenance, and other related activities such as training. The CDM APL is organized by CDM capabilities into five subcategories, one for each of the four CDM capability areas and a fifth for emerging tools and technologies.

  UPDATE: The CDM Tools Special Item Number (SIN) is retiring in 2022, however, approved CDM products are tagged on GSA Advantage! and available for purchase by federal agencies through CDM DEFEND, on IT Schedule 70, and from the NASA SEWP CDM Catalog. More information will be available soon.

- **CDM Request for Services (RFS) Process**
  The RFS is an acquisition tool designed to give flexibility to agencies over the life of a DEFEND contract. If a government agency identifies a new cybersecurity need that falls within or near a DEFEND requirement, they can submit a detailed and defined scope of work, or RFS, to help meet that need. CISA evaluates the request and, if deemed pertinent, the RFS is approved. The RFS is then issued to the respective DEFEND system integrator to begin performing the work.

- New CDM Dashboard Ecosystem Contract
  CISA awarded a six-year contract to provide a new government-wide dashboard for the CDM Program in 2019. Under this contract, the CDM Program has migrated to a new technology platform to deliver a solution that enables increased scalability, performance, flexibility, and innovation for agency customers.

For more information about the CDM Program, please contact the CDM Program Management Office at CDM@cisa.dhs.gov.