CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) PROGRAM

THE CYBERSECURITY AND INFRASTRUCTURE AGENCY (CISA) LEADS THE NATIONAL EFFORT TO DEFEND CRITICAL INFRASTRUCTURE AGAINST THE THREATS OF TODAY, WHILE WORKING WITH PARTNERS ACROSS ALL LEVELS OF GOVERNMENT AND IN THE PRIVATE SECTOR TO SECURE AGAINST THE EVOLVING RISKS OF TOMORROW.

PROGRAM OBJECTIVES

The Continuous Diagnostics and Mitigation (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; and
- **Streamline** Federal Information Security Modernization Act (FISMA) reporting.

CDM CAPABILITIES

The CDM Program delivers capabilities in five key program areas (Figure 1).

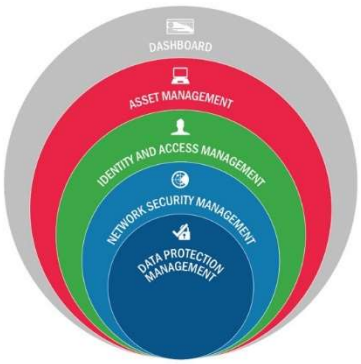

Figure 1: CDM Program Areas

- **Dashboard:** Receives, aggregates, and displays information from CDM tools at the agency and federal level.
- **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 Officer (CFO) Act federal civilian agencies. Those dashboards provide visibility on 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 IT managers to the most critical cybersecurity risks. In parallel to the deployment of agency-level dashboards, CDM has established the Federal Dashboard, 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 delivery model adheres to the core principles of a shared service, enabling agencies to leverage CDM tools and infrastructure to increase network security. The shared services approach is being deployed to government entities seeking a common platform across internal components or agencies lacking the infrastructure/resources for a standalone CDM implementation.

ACQUISITION STRATEGY

The CDM acquisition strategy is a two-pronged approach to provide products and services to meet the CDM program objectives. It includes 1) the CDM Tools Special Item Number (SIN) on GSA IT Schedule 70 and 2) services executed through the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND), a series of Task Orders (TOs) against the Alliant GWAC.

CDM TOOLS SIN 132-44

The CDM SIN is a government-wide contracting solution that provides a consistent set of Information Security Continuous Monitoring (ISCM) tools to federal, state, local, regional, and tribal governments. The SIN includes cybersecurity tools and sensors. CDM provides monthly opportunities to refresh and add new tools including innovative tools that meet the technical requirements of the CDM program via the CDM Approved Product List (APL).

CDM DEFEND

The scope of CDM DEFEND encompasses all activities that support CDM capabilities, along with the following:

- Deploys CDM capabilities across the .gov domain;
- Deploys the capabilities within groups of agencies to achieve volume discounts and other cost efficiencies;
- Provides flexibility for different requirements in terms of agency readiness, complexity, location of data (on premise/mobile/cloud), and mission objectives;
- Supports the use of innovative products; and
- Offers “shared service” options for agencies where sharing costs and skilled support yield most benefit.

CONTACT

For more information, visit www.dhs.gov/cdm (program information) or contact CDM@hq.dhs.gov