Homeland Security

CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

The growing numbers of cyber attacks on Federal Government networks are more sophisticated, aggressive, and dynamic.

Government computer networks and systems contain information on national security, law enforcement, and other sensitive data. It is paramount that the government protects this information from theft and protects networks and systems from attacks while continually providing essential services to the public and protecting individual privacy, civil rights, and civil liberties. The CDM program is a dynamic approach to implementing automated, risk-based cybersecurity that will better assure the security of sensitive data and the provision of essential functions while protecting sensitive information.

HELPING TRANSFORM RISK-BASED CYBERSECURITY

In support of government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity, the Department of Homeland Security (DHS) established the Continuous Diagnostics and Mitigation (CDM) Program, an implementation approach consistent with guidance from the Office of Management and Budget and the National Institute of Standards and Technology. CDM is a suite of capabilities and tools that:

- Enables network administrators to know the state of their respective networks at any given time;
- Informs on the relative risks of threats; and
- Makes it possible for system personnel to identify and mitigate flaws at near-network speed.

DHS, in partnership with the General Services Administration (GSA), established a government-wide acquisition vehicle (Blanket Purchase Agreement, or BPA) for continuous diagnostic capabilities. The purpose of the CDM BPA, which is available to Federal, state, local, and tribal government entities, is to:

- Provide a consistent, government-wide set of continuous diagnostic solutions to enhance the Government's ability to identify and mitigate the impact of emerging cyber threats; and
- Capitalize on strategic sourcing to minimize costs of continuous diagnostic implementation.

HOW CDM WORKS

The CDM Program enables Federal Government departments and agencies to expand their continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. CDM offers commercial off-the-shelf (COTS) tools, with robust terms for technical modernization as threats change. First, agency-installed sensors perform an automated search for known cyber flaws. Results feed into a local dashboard that produces customized reports, alerting network managers to their worst and most critical cyber risks, based on standardized and weighted risk scores. Prioritized alerts enable agencies to efficiently allocate resources based on the severity of the risk. Progress reports track results, which can be shared among sister networks. Summary information can feed into an enterprise-level dashboard to inform and prioritize cyber risk assessments.

Continuous Diagnostics and Mitigation Process Diagram

Homeland Security

IMPLEMENTATION OF CDM

DHS and GSA are structuring acquisition vehicles on behalf of CDM participants.

The CDM BPA is open to any government entity, including the Federal Civilian Executive Branch (.gov), as well as state, local, tribal, and territorial departments and agencies, and defense organizations. CDM BPA participants achieve cost savings through tiered-price and task order discounts, enabling more efficient use of scarce resources to be spread further. This strategy results in an enterprise approach to continuous diagnostics, including consistent application of best practices.

For Federal Civilian Executive Branch departments and agencies, DHS:

- Optimizes CDM acquisitions;
- Organizes Task Order participants;
- Buys sensors and services with DHS-appropriated funds for .gov departments and agencies;
- Provides services to implement sensors and agency dashboards for .gov departments and agencies; and
- Provides federal dashboard-related infrastructure.

State, local, regional, and tribal governments may use the Direct Order/Direct Bill option to procure products and/or services from the CDM Tools/CMaaS BPA via the delegated procurement authority, GSA Federal Systems Integration and Management Center (FEDSIM). For specific ordering options, please see GSA's CDM/CMaaS Ordering Guide, 2013, via **www.gsa.gov/cdm**.

BENEFITS OF CDM

The CDM Program better protects government networks through automated control testing and progress tracking. This approach:

- Provides services to implement sensors and dashboards in .gov departments and agencies;
- Provides near-real time results;
- Prioritizes the worst problems within minutes, versus quarterly or yearly;
- Enables defenders to identify and mitigate flaws at network speed; and
- Lowers operational risk and exploitation of IT systems and .gov networks.

HOW DHS IS MANAGING CDM

DHS ensures that the program is consistently implemented, meets critical requirements for effectiveness, and leverages centralized acquisitions to improve the speed of procurement and achieve strategic sourcing discounts.

The CDM Program Management Office (PMO) supports participating agencies through web-based toolkits, customer representative meetings, and agency-dedicated CDM advocates. The CDM PMO is housed in DHS's Federal Network Resilience Division within the Office of Cybersecurity and Communications.

For more information about CDM visit:
www.gsa.gov/cdm (ordering information)
www.dhs.gov/cdm (public website)

The CDM PMO offers a secure, community of interest for CDM participants, hosted on the Homeland Security Information Network (HSIN). To request membership, email the CDM PMO at **cdm.fnr@hq.dhs.gov**.

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets. For more information, please visit **www.dhs.gov/cyber**.