Homeland Security

Federal Network Resilience

CONTINUOUS DIAGNOSTICS & MITIGATION PROGRAM

The growing number of cyber attacks on Federal government networks are sophisticated, aggressive, and dynamic. A recent cybersecurity report* disclosed that over 90 percent of successful attacks require only the most basic mitigation techniques, and 96 percent of successful breaches can be avoided if simple or intermediate controls are put in place.

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 the Information Security Continuous Monitoring methodology. 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.

The CDM Program is a dynamic approach to fortifying the cybersecurity of computer networks and systems within agencies and across the Federal Government. DHS, in partnership with the General Services Administration (GSA), established a government-wide acquisition vehicle (Blanket Purchase Agreement, or BPA) for continuous monitoring 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 monitoring 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 monitoring implementation.

HOW CDM WORKS

The CDM Program enables Federal Government departments and agencies to expand their continuous monitoring capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. CDM will provide participants with:

- Agency-installed sensors that perform an automated search for known cyber flaws;
- Results that are fed into agency-level dashboards that produce customized reports, alerting IT managers to their worst and most critical cyber risks based on standardized and weighted risk scores;
- Prioritized alerts enabling agencies to efficiently allocate resources based on the severity of the risk; and
- Progress reports that track results which can be shared within agencies. Summary information will feed into a central DHS-managed dashboard to inform and prioritize cyber risk assessments across the Federal Government.

Continuous Diagnostics and Mitigation Process Diagram

*James A. Lewis, Raising the Bar For Cybersecurity, Center for Strategic and International Studies, Washington, D.C., 2013

Homeland Security

Federal Network Resilience

IMPLEMENTATION OF CDM

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/agencies; and
- Provides federal dashboard-related infrastructure.

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 agency dashboards in .gov departments/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 Federal 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 (CS&C).

For more information about CDM, visit **www.dhs.gov/federal-network-resilience** or email **cdm.fnr@hq.dhs.gov.**

ABOUT DHS CYBER

DHS is responsible for safeguarding the Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. As DHS is the lead agency on cybersecurity, the Office of Cybersecurity & Communications 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 on DHS cyber programs, visit **www.dhs.gov/cyber**.