Trustwave®

# Federal CDM Program Funds Continuous Monitoring Data Security Initiatives

## GET YOUR SHARE: $6 BILLION AVAILABLE TO .GOV FEDERAL AGENCIES

In 2012, the Office of Management and Budget identified continuous monitoring of federal IT networks as one of fourteen Cross- Agency Priority (CAP) goals, established in accordance with the Government Performance and Results Modernization Act.

To support federal departments and agencies in meeting the CAP goal, DHS established the Continuous Diagnostics and Monitoring (CDM) Program and Congress appropriated $6 billion to fund the acquisition of tools and services that enable federal and other government IT teams to strengthen the security posture of their cyber networks.

A key component of the CDM initiative is the protection of federal databases. This program brief can help your agency learn about taking advantage of this program to achieve the database security compliance requirements of the Continuous Monitoring initiative.


The CDM program enables government entities to expand their continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts.

## Requesting Funds

CDM funds are available to ".GOV" federal agencies to purchase approved CDM tools and services. In Phase 1, these include:

1. Hardware asset management
2. Software asset management
3. Vulnerability management
4. Configuration settings management.

Agencies should apply for funds now to ensure a proper allocation of resources, working with your agency's program manager to request the desired products. The PM will then add that request to the RFQ for a given task order.

## Prioritize Your Needs

To get started, agencies should begin prioritizing and identifying solutions they want to deploy for Continuous Monitoring, beginning with database security, which is central to the Continuous Monitoring mandate.

Ensuring federal databases have the latest security patches, strongest passwords, and properly configured settings and user privileges helps protect against cyber-attacks.

According to the Trustwave® SpiderLabs® Research team, "…most recent database updates are for vulnerabilities that are remotely exploitable without authentication. In other words, anybody on the network can exploit these vulnerabilities."

Moreover, database security scanning is not only a security best practice, it is recommended by the security and compliance guidelines defined by DHS in its Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS). Section 2.2.3.3 "Database Vulnerability Scanners" specifically calls out database vulnerability scanners as a key component of the Continuous Monitoring initiative.

CAESARS also specifically refers to Trustwave DbProtect as a potential solution to address database scanning. In fact, Trustwave DbProtect addresses two of the key areas identified in the CDM program, by delivering proven vulnerability assessment scans and configuration scans against your organization's database applications.

## Trustwave Database Protection

Trustwave DbProtect is a security platform designed for consistent monitoring and management of databases that:

- Uncovers database weaknesses including configuration mistakes, identification and access control issues, and missing patches
- Monitors and prevents "escalation of privileges" attacks, data leakage, denial of service, or unauthorized modification of data held within data stores
- Allows organizations to secure their relational databases and big data stores throughout the environment.

Trustwave database security solutions proactively secure enterprise applications at more than one hundred federal agencies by discovering, assessing, protecting, and auditing the database against rapidly changing security threats. By securing data at its source, Trustwave enables agencies to securely perform their missions while minimizing the vulnerability and exposure of their sensitive data. Trustwave is dedicated to serving federal government agencies and meeting the requirements unique to their environments.

As part of this commitment, Trustwave is the only vendor to have a full suite of database security solutions, including Vulnerability Assessment and Real-Time Monitoring and Auditing solutions that are Common Criteria certified. Trustwave is fully committed to assisting its agency customers meet their important CDM and DISA-STIG compliance requirements.

## For More Information

For more information on the CDM Program or for assistance in determining your database security and compliance needs, please contact the Trustwave CDM Program Manager at CDM@trustwave.com. For more information about Trustwave, visit www.trustwave.com.

Trustwave®

For more information: www.trustwave.com