

The Direction of the Continuous Diagnostics and Mitigation (CDM) Program

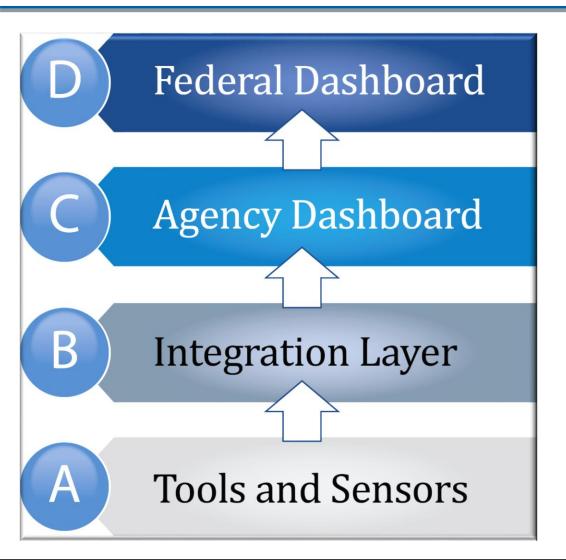
Cyber Resilience Summit October 16, 2018

CDM Program Capabilities

- Manage Assets
 - What is on the network?
- Manage Accounts
 - Who is on the network?
- Manage Network Security
 - What is happening on the network? How is the network protected?
- Manage Data Protection
 - How is data protected?



CDM Architecture



CDM architecture uses a four-layer design in which the "desired state" is compared to "actual state" data collected from CDM sensors in Layer A. Desired state policies are provided in the Federal Dashboard (Layer D) and Agency Dashboard (Layer C) and compared with actual state data in the CDM integration layer (Layer B).





GSA Alliant

Governmentwide Acquisition Contract (GWAC)

GSA Alliant 2

Governmentwide Acquisition Contract (GWAC)

DEFEND Task Order

Request for Services (RFS)

Group	Participating Agencies	DEFEND Prime Contractor
A	DHS	CACI
В	DOE, DOI, DOT, USDA, VA, OPM, EOP	Booz Allen Hamilton
С	DOC, DOJ, DOL, DOS, USAID, FCC, TVA	CGI Federal
D	HHS, Treasury, GSA, NASA, SSA, USPS	Booz Allen Hamilton
E	ED, HUD, HUD OIG, EPA, FDIC, NRC, NSF, SEC, SBA	ManTech
F	47 Small and Micro Agencies	TBD

GSA Schedule 70

CDM Tools Special Item Number (SIN) 132-44 170,000 + Products on CDM Approved Products List

> Agencies can use any purchasing method per FAR 8.405-1, including DEFEND

CDM Approved Product (APL) List Process

CDM PMO receives requests month to add, change or delete product families from the CDM APL. Package must include VPAT (508 compliance), GSA Approved Commercial Supplier Agreement Terms, & answers to supply chain management questionnaire.

3

CDM PMO ensures that all common & specific technical requirements are met by product family. CDM Products approved on the APL can be incorporated into a DEFEND RFS or procured directly by Agencies in accordance with the FAR.

1

Manufacturer adds product family & SKUs to GSA Schedule 70 Schedule holder submits product family package to CDM PMO to receive CDM SIN 132-44 CDM PMO evaluates package completeness CDM PMO reviews product technical capabilities CDM PMO approves CDM SIN designation GSA adds CDM SIN to product's schedule 70 & informs manufacturer

6

https://www.GSA.gov/cdm

CDM PMO publishes

updated CDM APL (monthly)



Moving Toward Threat-Based Risk Management

From Compliance to Threat-Based Risk Management

Cyber Hygiene



Compliance



Pre-CDM

- Manual FISMA compliance
- Yes/no responses are simplistic
- · Risk determination based on checklist

CDM Phases 1 & 2

- Automated asset management
- Automated account management
- Risk indicator scoring integrates automated data

Threat-Based Approach



CDM All Phases

- Visual dashboard reporting
- AWARE scoring prioritizes worst problems for mitigation
- Performance-based measurement

CDM Dashboards will enhance cybersecurity by providing a more standardized system that focuses on asset-based risk management, rather than compliance reporting.

