

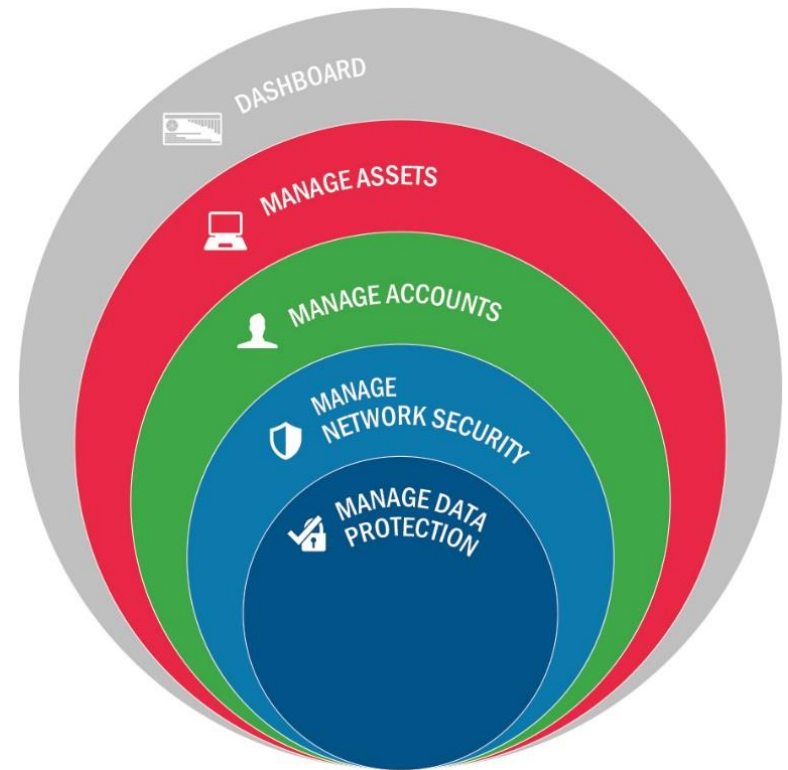


# The Direction of the Continuous Diagnostics and Mitigation (CDM) Program

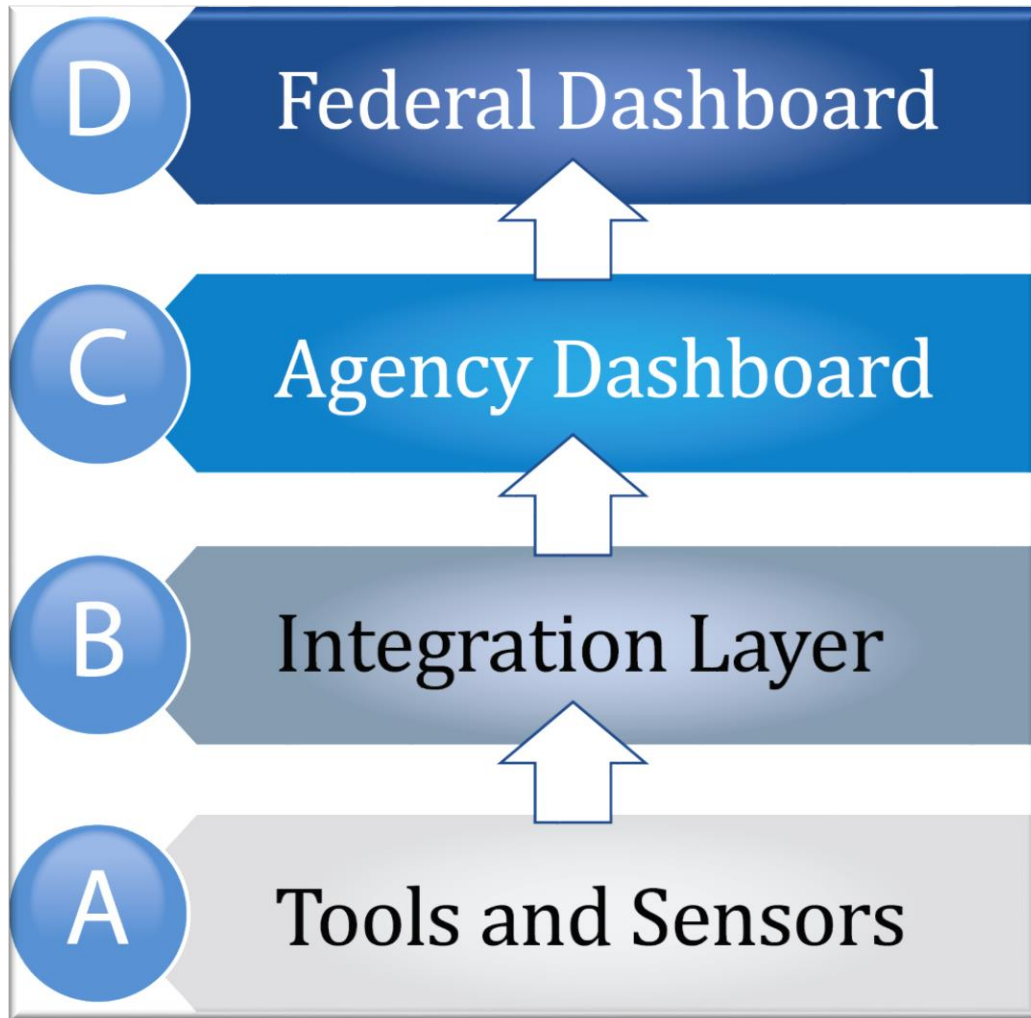
*Cyber Resilience Summit  
October 16, 2018*

# 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).



# CDM Program Acquisition Components

**GSA Alliant**  
Governmentwide Acquisition Contract (GWAC)

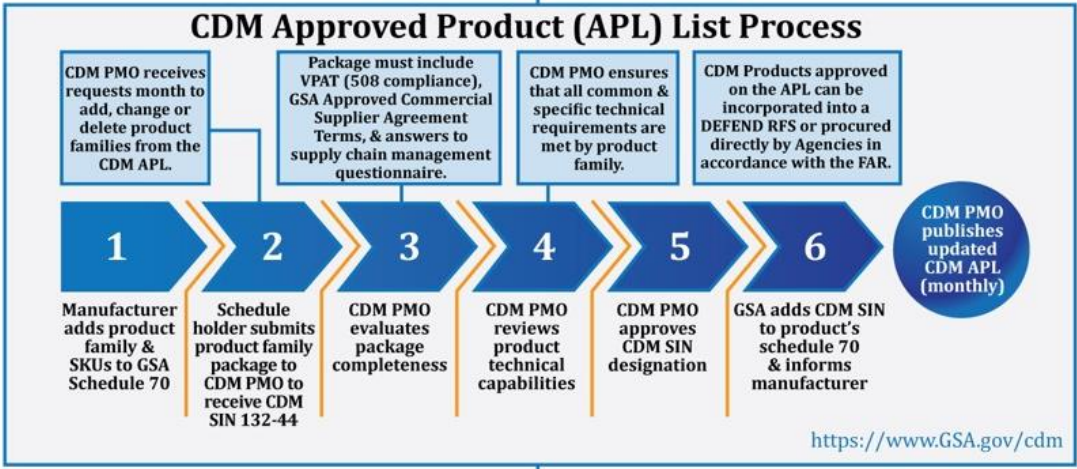
**GSA Alliant 2**  
Governmentwide Acquisition Contract (GWAC)

**DEFEND Task Order**  
Request for Services (RFS)

**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

Group	Participating Agencies	DEFEND Prime Contractor
A	DHS	CACI
B	DOE, DOI, DOT, USDA, VA, OPM, EOP	Booz Allen Hamilton
C	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



# Moving Toward Threat-Based Risk Management

## From Compliance to Threat-Based Risk Management

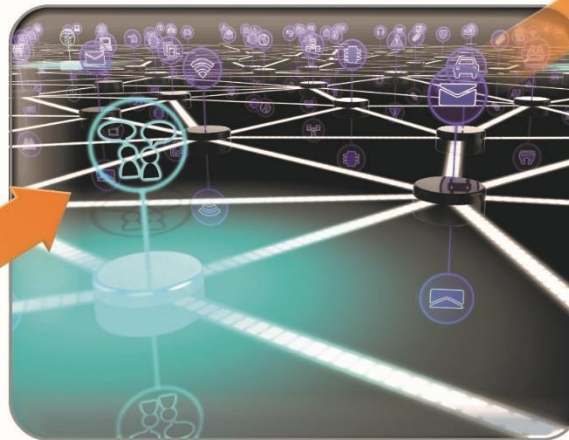
### Compliance



### Pre-CDM

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

### Cyber Hygiene



### 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.

