CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM: THE NEXT FRONTIER

CISQ CYBER RESILIENCE SUMMIT
CDM Program Capabilities

Agency and Federal Dashboards
Visualization tool to better understand, prioritize, and mitigate cyber risks.

Asset Management
What is on the network?

Identity and Access Management
Who is on the network?

Network Security Management
What is happening on the network? How is the network protected?

Data Protection Management
How is data protected?
## CDM Program Architecture

<table>
<thead>
<tr>
<th>Level</th>
<th>CDM Goal</th>
<th>Capabilities</th>
</tr>
</thead>
</table>
| Federal Dashboard Ecosystem | Government-wide visibility and analytics | • Government-Wide Visualization / Reporting  
• Threat Intelligence Informing Risk  
• Stack Health Monitoring  
• Government-Wide Analytics  
• Orchestrated Requests for Information  
• Threat Intelligence / Information Dissemination  
• Data Analysis and Event Management |
| Agency Dashboard Ecosystem | Agency-wide visibility and analytics | • Enterprise-Wide Data Aggregation and Normalization to common data schema  
• Standardized Risk Scoring  
• Incident Response Reporting  
• FISMA Reporting  
• Enterprise-wide Ongoing Assessment  
• Data Analytics / Machine Learning |
| Data Collection and Normalization | Full stack management | • Hardware Asset Management  
• Software Asset Management  
• Configuration Settings Management  
• Vulnerability Management  
• Identity and Access Management  
• Network Security Management  
• Data Protection Management  
• Mobile Data Management  
• Cloud Asset Management  
• Incident Response  
• Ongoing Assessment / Authorization |

**Key** = Existing Capabilities  Future Capability Under Consideration
COVID-19 and CDM Impact

- Assess, identify, and monitor programmatic risks related to COVID-19
- Support agencies' ability to telework at scale on both cloud and mobile environments
- Adjust delivery and implementation processes of CDM capabilities; continue to make progress in supporting agencies with CDM deployments
- Supported two agencies in strengthening their cloud security and security operations capabilities
- Continue to keep our staff safe during this time, as they work to provide a critical service
- Continue to explore the best approaches for working and communicating with our partners and stakeholders in a virtual environment
CDM Areas Where Progress Continues to be Made

- Asset Management Gap Fill
- Identity and Access Management Gap Fill
- Deployment of New Dashboard
- Implementation of Data Quality Management Certification Process
- Operationalization of Agency-Wide Adaptive Risk Enumeration (AWARE)
- Continuation of Data Protection Management Pilots
- Continuation of Cloud and Mobile Security Implementation
FY 2021 Priorities

These priorities are in addition to ongoing Data Quality efforts

**Asset Management and Identity and Access Management Gap Fills**
Continue existing work to complete gap fills for Asset Management and Identity and Access Management capabilities

**Mobile Asset Management**
Following mobile asset discovery completion, integrate mobile asset management to the Agency Dashboard

**CDM Dashboard Ecosystem**
Transition agencies to more scalable, capable, and flexible dashboard ecosystem

**Cloud Security Pilots**
Following cloud discovery completion, work with agencies, system integrators, and industry partners to determine the right approach and scope for cloud security pilots

**High Value Assets (HVA)**
Expand HVA pilots at additional agencies to extend data protection capabilities; explore the possibility of having at least one pilot per DEFEND group
CDM Program Values

LEADERSHIP
requires Technical Excellence and Open Communication

ACCOUNTABILITY
requires Transparency and Consistency

PARTNERSHIP
requires Flexibility, Timeliness, and Fairness
DO YOUR PART.
#BECYBERSMART
CISA.gov/cyber-month

NATIONAL CYBERSECURITY AWARENESS MONTH 2020
For more information:

[cisa.gov/cdm](https://cisa.gov/cdm)

CDM Program Questions?

Email: [CDM@cisa.dhs.gov](mailto:CDM@cisa.dhs.gov)