CDM PROGRAM WILL COMBAT CYBERTHREATS

CYBERTHREATS REMAIN A SERIOUS PROBLEM

Government organizations have the lowest security scores across all sectors.

Government has the highest number of incidents due to Denial of Service (DoS), policy violations, malicious code and improper usage.

Federal data breaches were at their highest level in 2015. Four major national government organizations were breached in 2016.

GOVERNMENT HAS TAKEN STRONG ACTION

DHS and GSA launched the Continuous Diagnostics and Mitigation (CDM) program, which is being adopted widely across government.

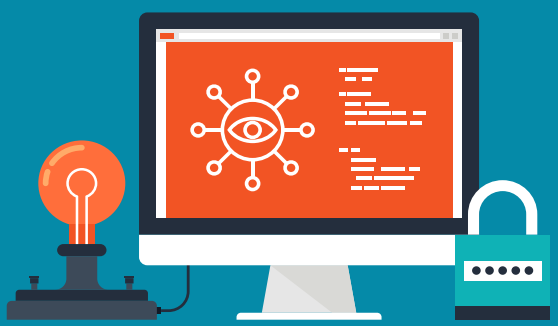
The federal FY2017 budget allocates more than $19 billion for cybersecurity, a 35% increase over FY2016.

The federal FY2017 budget increases CDM funding specifically by nearly 169%, to $173.3 million.

CDM HELPS AGENCIES MANAGE CYBERTHREATS

CDM WILL PROTECT GOVERNMENT NETWORKS BY:

1. Automating control testing and progress tracking
2. Accurately identifying risks
3. Understanding the state of networks at all times
4. Simplifying integration of security tools
5. Improving visibility into endpoint, network and security devices
6. Prioritizing security issues quickly using sensors and dashboards
7. Fulfilling FISMA requirements

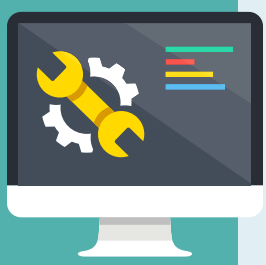


GOVPLACE

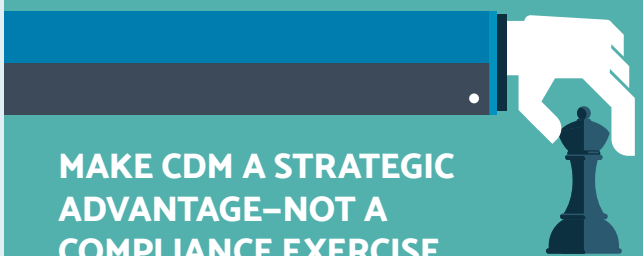
To get the real benefits of CDM, agencies should take a holistic approach in which tools are fully integrated.

CDM COMPLIANCE IS ONLY THE BEGINNING

LEVERAGE THE CDM BPAS FOR ACCELERATED SECURITY ADVANCES



- The BPAs provide easy access to a core set of tools that can be tailored to meet an agency's specific cyber requirements
- The volume discounts negotiated by GSA provide significant cost savings over open market pricing
- Cut out the middleman: Order directly off the BPAs by getting a Delegation of Procurement Authority from GSA



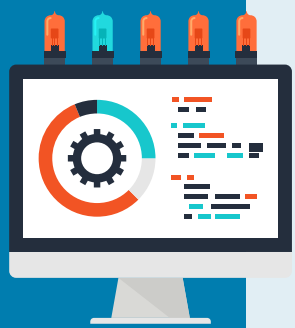
MAKE CDM A STRATEGIC ADVANTAGE–NOT A COMPLIANCE EXERCISE

- Begin with compliance: It's the best way to ensure that you don't get forced to follow someone else's tech refresh plan
- Implementing a cyber strategy that focuses on compliance can lead to a piecemeal approach that masks underlying vulnerabilities
- The CDM Readiness and Planning Guide can help you leverage CDM as a foundation for a more holistic cyber strategy

A HOLISTIC METHOD ADAPTS TO NEW THREATS

YOU GOT THE FOUNDATION… THEN EVOLVE

- The CDM Shared Services Platform provides improved security, helping agencies with limited budgets to meet the requirements of phases 1 and 2
- Additional modules or features can extend CDM to meet unique or emerging requirements of your environment
- The evolution of the cyberthreat landscape is shifting the focus from network protection to data protection that requires enhanced CDM security features



STRENGTHEN YOUR CYBER POSTURE THROUGH THE SMART USE OF CDM DATA

- Use data gathered through the CDM initiative to align future cyber spending with your specific cyber requirements
- Conduct flash assessments using CDM data collected in phases one and two to lay the groundwork for connecting to intelligence-driven programs such as EINSTEIN
- And don't go it alone: GovPlace can help you implement best practices from public and private R&D communities, taking full advantage of existing, new and emerging cyber technologies

For more information, please visit: www. govplace.com