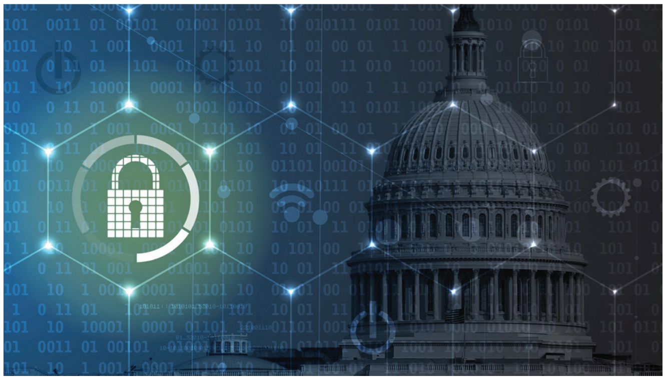
MeriTalk
Improving the Outcomes of Government IT

CDM is Evolving. What's Next?

Author: Jean Edwards, Managing Director, Business Development, Civilian Agencies, Federal Strategic Programs, Dell EMC



OMB's Risk Report raised the cyber flag again – 71 of 96 federal agencies are missing "fundamental cybersecurity policies" or have "significant gaps" in their cybersecurity programs. There is no silver bullet, but the Continuous Diagnostics and Mitigation (CDM) program provides an opportunity to continually improve cybersecurity risk postures across the federal government.

During CDM's first phases, agencies identified the assets and users on the network. Coming up next, the third and fourth phases will focus on proactively identifying cybersecurity risks. The goal is to close the gaps and ultimately enable agencies to prevent attacks.

As agencies work to secure on-premise, cloud, and hybrid environments, CDM is evolving – drawing on lessons learned around procurement, risk scoring, and the importance of visibility into cybersecurity maturity.

DEFEND and AWARE Move Toward Perfecting the Process

DEFEND – Dynamic Evolving Federal Enterprise Network Defense – aims to improve acquisition practices across all CDM phases. DEFEND will expand task orders, increase contract ceilings, and require integrators to consider data quality from the start of each contract to minimize inconsistencies among vendors. Importantly, the new acquisition strategy uses a cost-plus method, encouraging vendors to achieve all requirements.

DHS is also developing the Agency Wide Adaptive Risk Enumeration (AWARE) scoring algorithm. AWARE will help agencies assess key cyber risk issues including patching and network configuration to determine the most critical vulnerabilities. The goal is to enable agencies to prioritize and address priority threats first, track progress, and manage mitigation. In the future, AWARE will serve as a consistent, objective risk measurement tool for monitoring and comparing cyber exposure, giving agencies strategic insight across agencies and departments.

Raising the Grades

The CDM program is designed to shine a light on cyber best practices and help agencies make better decisions by identifying reliable solutions, taking the guess work out of acquisitions. Leveraging these tools, agencies can meet FISMA cyber requirements – key to improving grades on the newest category of the FITARA scorecard. For example, 18 out of 24 agencies received a D or F for this category on the most recent scorecard – more work ahead.

One Part of a Larger Conversation

Highlighting the importance of these efforts, over the summer, Rep. John Ratcliffe (R-Texas) introduced new CDM legislation "to advance and modernize" the program. If passed, the bill will ensure agency tools remain current as technology advances.

At Dell EMC, we believe CDM efforts must be a top priority for every agency. We view CDM as a permanent capability, not just a program that ends when the phases are complete. CDM is not a compliance checklist, but part of the larger cybersecurity conversation that includes technology, strategies, and best practices. Taking advantage of CDM is a vital step toward shifting the stance from reactive to proactive – preventing cyber breaches and data loss.

As a leader across the full cybersecurity ecosystem, Dell EMC supports federal customers within and beyond the CDM phases. We deliver comprehensive data protection solutions, and we are focused on all aspects of the cyber landscape, including the full supply chain, and the importance of building NIST and ISO-compliant hardware.

We know the key word is "continuous." And continuous cyber success drives continuous mission success. As we move forward together, there is a real opportunity to strengthen our cyber defenses and progress within, and beyond, the CDM program.

Read more about our data protection solutions: https://www.dellemc.com/en-us/data-protection/index.htm#scroll=off.

Learn more about our federal capabilities: https://www.dellemc.com/en-us/industry/federal/federal-government-it.htm.

Sponsored by:

DELL EMC