FEDInsider

DATASHEET

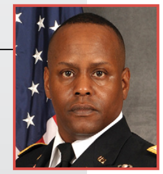
CLOSING THE GAP:
CDM's Role in Government During Teleworking

Contributors:

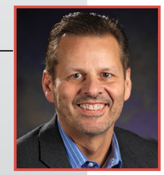
- **Hemant Baidwan**
  Deputy CISO,
  DHS, OCIO

- **Vijay D'Souza**
  Director, IT & CS
  GAO

- **William Robinson II**
  CTO & Sr. Technical Advisor, U.S. Army



- **Marcel Shaw**
  Principal Federal Solutions Architect,
  Ivanti



In response to the COVID-19 pandemic, most federal agencies needed to evolve their policies and best practices in order to safely operate within a new working environment that centered on telework. And as more federal employees have been forced to telework, agencies have had to implement new security measures to protect sensitive data. One of the best assets for doing this is Continuous Diagnostics and Mitigation (CDM). Created by the Cybersecurity and Infrastructure Security Agency (CISA), CDM is comprised of a series of principles, best practices and commercial tools that can be used to build and maintain a strong security posture at agencies.

The CDM program offers agencies tools to improve their security such as commercial dashboards that compile actionable intelligence about security threats for agency decision makers. With no sign of government teleworking ending anytime soon, it's worth examining all four tenets of CDM including asset management, identity and access management, network and security management, and data protection. The following are four takeaways from government and private sector experts about how CDM can help bolster federal cybersecurity.

1. CDM Improves and Focuses Federal Security across the Enterprise

Security, by its nature, requires collaboration and proactivity in order to operate at the highest level. Security within the public sector is no exception as multiple agencies need to ensure that their defenses are strong enough to protect sensitive government information from hackers and threat actors. This has led numerous federal agencies to institute CDM to improve their security framework and develop mitigation strategies.

"I'm proud of the partnership [with CISA and other agencies] in helping to continue that mission," said Chief Warrant Officer 5 William Robinson, Chief Technology Officer and Senior Technical Advisor for the Department of the Army. "So overall, I would say it has allowed us to further strengthen our secure posture and provide us a wider understanding of the risks, and in implementing the most effective tools and practices within the department internally."

Having information about active threats readily available, and sharing that data with other federal agencies using CDM tools helps to strengthen government networks across the board. It supports efforts by providing a unified defense against an increasingly complex threat landscape, Robinson noted.

2. Asset Management Is a Critical Pillar of CDM for Most Agencies

With such large enterprises, the asset management pillar of CDM is often the first one that most agencies decide to tackle. Managing software and hardware is critical in helping maintain mission readiness, especially with so many telecommuting and remote employees. Thankfully, many of the CDM tools available to agencies are designed to streamline and automate complex asset management.

"I think agencies are definitely headed in the right direction," said Vijay D'Souza, Director, Information Technology and

Cybersecurity for the Government Accountability Office (GAO). "Asset management was probably one of the trickiest things we found."

D'Souza says that CDM is helping agencies by providing tools and benchmarks that collect information about assets, and then rolling all of that information up into one place. In a lot of ways, good asset management is the core to protecting everything else.

"For asset management, being able to better see yourself is always a critical component in being able to understand what is out there," Robinson said. "Now we're better able to map and secure those things, and that's also important for standardization."

3. CDM Is Best Deployed Using a Layered Approach

Implementing a new program across all of government can be difficult due to the tangled web of legacy and enterprise systems deployed throughout federal agencies. Instead, experts recommend that agencies focus on certain aspects of CDM and implement them individually and over time to avoid disruptions.

"You really need to deploy in stages because it's a layered approach," said Marcel Shaw, Federal Solutions Architect at Ivanti. "The management processes need to be implemented, and they need to be accurate. So think of hardware and software asset management as prerequisites to configuration management and vulnerability management."

For CDM to work at the highest levels of government, it's important for agencies to realize the order of implementation. "So if you look at it in phases, then in phase one you're managing assets," Shaw said. "Then you start managing events and finally move into data protection."

While every agency deployment is different, they should all be done in phases according to Shaw. A cautious approach to CDM will yield the best results with the least disruption.

4. Maintaining Cybersecurity in a Teleworking Environment

Almost every government agency needed to adapt to a telework heavy environment early into the COVID-19 pandemic. While most agencies had a telework option for some civilian jobs, few agencies had robust enough infrastructure to handle the high percentage of employees who were forced to telework once the pandemic struck. While improving the federal infrastructure has gone relatively smoothly, agencies also have had to worry about potential new security issues with so many employees working from home.

"I think the biggest issues have been at agencies where the jobs weren't designed for telework," said Hemant Baidwan, Deputy CISO for the Department of Homeland Security. There are a lot of dangers in a home office that simply don't occur inside an agency.

"For example, everyone has smart speakers now, and if you're on this phone call and you have Siri sitting next to you, do you need to disable it?" Baidwan asked. "We've talked about situations like that, and reminded people to be wary of things that they don't always think about."

CDM can help protect government during massive teleworking in two ways, according to Baidwan. First, it can add an extra layer of visibility to federal networks so that if a previously unknown security threat occurs, it will be easy for agency IT personnel to quickly learn about it. And the CDM tools can also enforce policies, like restricting telecommuting employees from connecting to government networks through public Wi-Fi.

Even though CDM is a relatively new program, the technology, policy, dashboards and other assets and tools provided through it are already helping to secure government agencies. So long as it is carefully implemented and maintained, it can continue protecting and securing federal networks, even during unprecedented changes like the shift to teleworking.

Hosky Communications Inc.

3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300

Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

ivanti

10377 South Jordan Gateway, Suite 110
South Jordan, Utah 84095
Marcel Shaw, *Principal Federal Solutions Architect*

(703) 624-0907

Marcel.Shaw@Ivanti.com
www.invanti.com/
Facebook.com/GoIvanti
Linkedin.com/company/Ivanti/
@GoIvanti