Agencies Incorporate CDM

Officials look for ways to integrate cybersecurity into existing efforts while addressing a growing threat surface.

With the goal of bolstering cybersecurity across the entire government, Homeland Security established the $6 billion Continuous Diagnostics and Mitigation (CDM) program to evaluate tools to perform those functions. Agencies can then procure them through the General Services Administration. Challenges have emerged, however, as agencies work to integrate CDM into existing cybersecurity measures.

First, the thought was 2 million assets existed government-wide. That number is actually twice as high, as agencies discovered after CDM reported they should have knowledge of all IP addressable devices, says James Quinn, lead systems engineer for CDM at DHS, during a panel discussion titled "Continuous Diagnostics & Mitigation: Fortifying Government." Suddenly, the attack surface was much larger.

> "We now have a firm grasp on identify, but now **we have more things** that we have to look at to protect."
>
> **JAMES QUINN,**
> **LEAD SYSTEMS ENGINEER FOR CDM AT DHS**

The first two of CDM's three phases emphasize this issue of identifying assets. "Phase I and Phase II were the would've, could've, should've because it's a problem everyone was supposed to have solved 10 years ago," says Quinn. "It was a $200 million problem across the .gov space that people did not have the money or the ability to focus on. The downside is we now have a firm grasp on identify, but now we have more things that we have to look at to protect."

At the Justice Department (DOJ), prioritizing and integrating CDM into existing cyberinitiatives hasn't always been easy, says Brian Depasse, DOJ's assistant director for cyber engineering, architecture, and identity management. To ease those pain points, he and his team work closely with DOJ's downstream components as well as the CDM program office to ensure they are efficient and getting support from leaders.

From the vendor perspective, there is friction between the security and infrastructure sides of the IT shop, but a visibility platform that serves traffic to both of those can help, says Tom Kopko, senior director for federal civilian agencies at Gigamon. "Visibility serves both security and infrastructure in the exact same way by delivering the right information to cybersecurity tools or network management tools or application management tools, both from a data center perspective and also into the cloud," he says. "The right visibility platform brings all that stuff together, so that any data, no matter where it reaches the platform can be secured or analyzed by any tool, whether it be on-premises or in the cloud."

The National Cybersecurity Center of Excellence is working to alleviate some of the problems agencies face with CDM, says Tim McBride, the center's acting deputy director. It's a place where industry, academia and government can come together resolve issues. For example, the center has established a generic instance of CDM used for demonstrations and to help inform how things are going.

Other helping hands come in the form of using Schedule 70 for CDM-certified products and upcoming task orders called DEFEND, which will be awarded this fiscal year. "That gives agencies the ability to use more competitive structure for them to build products, and know those products are on our approved product list and therefore meets the capabilities for being integrated into the CDM environment," says Quinn.

The Navy doesn't use CDM. However, but the program it does use essentially validates the entire CDM approach, says Thresa Lang, deputy director of the service's Cybersecurity Division. In 2014, the chief of naval operations stood up a task force to focus on cybersecurity. From that came the CYBERSAFE program, which led to the Cybersecurity Division, now part of the CIO division.

"In 2014, we also adopted the Cyber Security Framework from [the National Institute of Standards and Technology], and we have found that it's extremely useful for us in helping prioritize our spend and making sure that we have cybersecurity as the primary thing that we look at before we start making financial tradeoffs," says Lang. The Navy reprioritized more than $300 million of its budget to address cyberresiliency.