

## Why Agencies Should Focus on CDM Outcomes, Not Tools

Implementing continuous diagnostics and mitigation requires a holistic approach to integration.

[James Mersol](#)

Fri, 10/18/2019 - 13:44



Photo Credit: matejmo/iStock

The federal government's continuous diagnostics and mitigation (CDM) program is being implemented across 33 different federal agencies, each with their own missions, capabilities and approaches. With all the roadblocks presented with tools, funding and networking integration, agency leaders are discussing lessons learned for paving the way forward.

For the Small Business Administration, focusing on the outcomes instead of the tools led to successful CDM implementation.

“When CDM was rolled out, it was very tool based,” said Maria Roat, CIO for SBA during the Oct. 10 MeriTalk CDM Central event. “It was very focused on the tools, but not necessarily on the outcomes and the intent of CDM.”

Because SBA ran a pilot program for CDM this summer, it was able to try things differently, like running the CDM tools in the cloud.

“I’ve got a multi-cloud environment, and I knew that the current CDM platform was not going to meet my needs,” Roat said. “I had 40 tools — I got rid of those, and I’m down to about 10 right now. I’m using cloud-based tools to manage my entire network ... I can see that entire footprint across my entire enterprise for all of my users wherever they are.”

Even though those tools were not what the original CDM dashboard had in mind, the outcome hits all four CDM phases — knowing what is on the network, who is on the network, what activity is happening on the network and how data is protected.

“It’s about the data it’s about the outcome, and it’s about the intent of CDM,” said Roat. “We’re showing the capabilities of what you can do, and we’re challenging CDM.”

“It’s very easy to go off on the CDM ‘path’ unilaterally,” said Gary Stevens, deputy CIO and director of cyber strategy for the Department of Veterans Affairs. “It has to be part of a holistic front.” Stevens said one of his initiatives at VA is to ensure that CDM fits into the larger cybersecurity architecture of the agency.

Stevens also recommended thinking about the CDM framework as “guideposts” for the desired capabilities, thinking above all about how it ties into each agency’s initiatives and goals.

“Security is all about enabling the mission,” he said. “For us, it’s crucial that we do that as we move out on the integrated health record, the digital transformation [and] the modernization efforts.”

Like Roat, Stevens said focusing on the intent of directives like CDM and NIST guidelines will deliver the most value for agencies.

“I think there’s an attempt to try and conform to the spirit or the specific language within the security controls,” he said. “And really, it’s all about how you satisfy the intent of that control through a multitude of means and how you manage that from a risk standpoint.”

The CDM-approved products list now includes over 245,000 approved tools for agencies to use, giving them the freedom to find a solution that delivers the desired outcome, but does not negatively affect the mission. CDM Program Manager Kevin Cox reassured agencies worried about quality and security that every one of these approved products has been properly vetted and that the Department of Homeland Security and General Services Administration will continue to review them.

“We’re working to bring in additional criteria to ensure that the products that are on the approved products list have good information related supply chain,” he said. “We do have information that can inform agencies as they’re looking to use particular products within CDM.”

The impact and effects of CDM will be the program’s next focus, he added.

“In fiscal years 2019 and 2020, we really need to focus on the operationalization of CDM,” said Cox. “It’s about getting the value of getting the tools out there, but [also] being able to utilize the data coming up from those tools to really help inform agency processes.”

[View printer friendly version](#)

[CDM](#)

[Veterans Affairs](#)

[Federal Cybersecurity](#)

[SBA](#)

[Department of Homeland Security](#)

[Standard](#)