CDM SHARED SERVICES PLATFORM: PROVIDING ACCESS TO SMALLER FEDERAL AGENCIES

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. The Continuous Diagnostics and Mitigation (CDM) Program provides federal agencies with cybersecurity tools, capabilities, and services that enable persistent visibility and expedited reduction of risks.

The CDM Shared Services Platform (SSP) provides 75 eligible non-Chief Financial Officers (CFO) Act agencies with access to CDM cyber capabilities and a CDM Dashboard through a multi-tenant, cloud-based shared service delivery model. This solution has been tailored to mitigate small and micro-agency resource constraints (e.g., funds and personnel). Using the shared services approach results in cost savings from lower cost of ownership, amount of equipment needed, and associated labor at each participating agency. All software licenses associated with the CDM Shared Services Platform are covered by the CDM Program Management Office. Deployment is rapid (three months on average), with the CDM Program providing a system integrator for deployment assistance and training.

"Our agency is so small that our license needs typically don't meet the vendor minimum requirements for purchasing, so we would not be able to afford and deploy these state-of-the-art tools without help from the CDM Shared Services Program," said Grace Kim, an Information Technology Specialist at the National Capital Planning Commission (NCPC), one of the agencies taking advantage of the CDM SSP.

CDM's automated tools and services streamline the NCPC's capabilities and are essential to the agency's move to a modern zero trust environment, a security framework that requires all users inside and outside of a network to be continuously validated before being provided access, according to Kim. She noted that two capabilities offered through the SSP also helped her agency secure remote assets when it transitioned to a full telework environment. "We're able to scan and patch assets from the cloud in real time and no longer have to rely on users to connect to the [Virtual Private Network] VPN," Kim said.

When it comes to federal data calls requiring a quick turnaround, the CDM Dashboard's data has helped the NCPC provide information on everything from a list of critical software to known exploitable vulnerabilities. "We're piloting the automated data call feature [of the CDM Agency Dashboard], which is very promising," Kim said.

The Federal Maritime Commission is another example of a small agency that has benefited from the SSP. Chief Information Security Officer Greg Francis said, "As an early adopter of the CDM Program,

my agency and I are extremely pleased to be a member of the CDM-F program," referring to the CDM Program's program designation of Group F for the SSP offering. "The benefits of the CDM Program have been immeasurable to my non-CFO Act small agency," he said, noting that the Commission relies on the capabilities to identify system vulnerabilities and to prioritize remediation based on severity. "The [Vulnerability Management, Detection, and Response] VMDR and the threat detection function in [the CDM capability offered through the SSP] provide the very comprehensive look at the vulnerabilities that are present in my environment and on which systems. It has, as I said, been immeasurable to our ability to respond to [Binding Operational Directives] BODs, to identify the various [Known Exploited Vulnerabilities] KEVs and remediate them in our environment."

Moving forward, the CDM Program's focus is to optimize the use of the data provided to CISA to help agencies quickly and easily report their progress on BODs.

To learn more about CDM SSP 2.0, please contact cdm@cisa.dhs.gov.

For acquisition-related questions related to the CDM SSP 2.0, please contact csd_cb.acqbudg@cisa.dhs.gov.