WRITTEN TESTIMONY OF STEPHEN ZAKOWICZ

VICE PRESIDENT

CGI FEDERAL INC.

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY

"Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs"

SEPTEMBER 19, 2023

INTRODUCTION

Chairman Garbarino, Ranking Member Swalwell, and other distinguished members of the Subcommittee on Cybersecurity and Infrastructure Protection, my name is Stephen Zakowicz. I am a Vice President at CGI Federal Inc. ("CGI Federal"). As a wholly-owned U.S. operating subsidiary of CGI Inc. ("CGI"), [1] CGI Federal and its 7,100 employees partner with federal agencies to provide solutions for homeland security, defense, civilian, healthcare, justice, intelligence, and international affairs. During the last four years, I have served as the Project Manager on CGI Federal's contract with the Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") for the Continuous Diagnostics and Mitigation ("CDM") Program. On behalf of CGI Federal and its employees, I am pleased to submit this written testimony to the Subcommittee regarding the CDM Program.

CDM is a mission critical federal program that provides participating agencies with solutions and services to identify and combat cybersecurity risk. Since its original contract award in 2016, CGI Federal has provided this support to 100 participating agencies through tailored solutions and a robust shared services platform. CGI Federal is currently the prime contractor on two CDM Dynamic and Evolving Federal Enterprise Network Defense ("DEFEND") Task Orders - DEFEND C and DEFEND F. Under its DEFEND C Task Order, CGI Federal provides tailored CDM solutions to seven large Federal agencies: Department of Commerce ("DOC"), Department of Justice ("DOJ"), Department of Labor ("DOL"), Department of State ("DOS"), Federal Communications Commission ("FCC"), Tennessee Valley Authority ("TVA"), and United States Agency for International Development ("USAID"). Under its DEFEND F Task Order, CGI Federal developed a state-of-the-art cloud-based Shared Services CDM platform, and currently operates and provides access to that platform to 65 non-Chief Financial Officer Act ("CFO Act")

[1] 1 Founded in 1976, CGI is among the largest independent information technology ("IT") and business consulting services firms in the world. With 90,250 consultants and professionals across the globe, CGI delivers an end-to-end portfolio of capabilities from strategic IT and business consulting to systems integration, managed IT and business process services, and intellectual property solutions. CGI works with clients through a local relationship model complemented by a global delivery network that helps clients digitally transform their organizations and accelerate results.

federal agencies. Roughly 300 CGI Federal employees and subcontractors support the CDM program.

CDM: Current Program Structure

As stated in the DHS FY24 Congressional Budget Justification for CISA, "the CDM program provides the Department, along with other Federal agencies, with capabilities and tools to identify cybersecurity risks to agency networks on an ongoing basis. It prioritizes these risks based on potential impacts and enables cybersecurity personnel to mitigate the most significant problems first… Furthermore, CDM enables CISA and agencies to proactively respond to threats through the deployment of multiple different security capabilities, including data protection technologies, Endpoint Detection and Response (EDR), cloud security platforms, and network security controls, and enables CISA to continually evaluate the cybersecurity posture of [Federal Civilian and Executive Branch ("FCEB")] systems and networks."

As CISA describes on their public website, the CDM program is structured to provide cybersecurity protections and capabilities in four key areas:

- The Asset Management (AM) capability is aimed at providing agencies with a centralized overview of their network devices and the risks associated with such devices. Asset Management enables an agency to maintain and improve its cyber hygiene through five capabilities: hardware asset management (HWAM), software asset management (SWAM), configuration settings management (CSM), vulnerability management (VUL), and enterprise mobility management (EMM).
- The Identity and Access Management (IDAM) capability is intended to manage the access and privileges of agency network users. Managing who is on the network requires the management and control of account and access privileges, trust determination for people granted access, credentials and authentication, and security-related behavioral training.
- The Network Settings Management (NSM) capability is designed to provide agencies with greater visibility into what is happening on their networks, which also gives them a better understanding of how the networks are being protected.
- The Data Protection Management (DPM) capability is intended to provide additional protections to the most critical mission data and systems on federal civilian networks. While the other CDM capabilities provide broader protections across federal networks, the DPM capability is focused on protecting sensitive (especially private) data within the agency.

These capabilities are centrally managed and reported through the CDM Dashboard Ecosystem, a cloud-based visualization and data analytics layer that allows agencies and CISA to obtain a top-level view of cybersecurity risk posture and access details regarding how individual systems and endpoints contribute to that risk posture. This allows agency personnel to quickly identify and address the highest risk cybersecurity vulnerabilities first.

The current CDM program consists of seven individual Task Orders to provide consistent, prioritized CDM capabilities to FCEB agencies. Those Task Orders are:

- CDM DEFEND A: Providing CDM program requirements to DHS
- CDM DEFEND B: Providing CDM program requirements to DOE, DOI, DOT, OPM, USDA, and VA

- CDM DEFEND C: Providing CDM program requirements to DOC, DOJ, DOL, DOS, FCC, TVA, and USAID
- CDM DEFEND D: Providing CDM program requirements to GSA, HHS, NASA, SSA, and Treasury
- CDM DEFEND E: Providing CDM program requirements to DOED, EPA, FDIC, HUD, NRC, NSF, SBA, and SEC
- CDM DEFEND F: Providing CDM program requirements to up to 75 small and medium FCEB agencies through a Shared Services platform
- Dashboard Ecosystem: Developing and hosting a common CDM Dashboard platform on behalf of CISA to receive and consolidate information from participating CDM DEFEND agencies

CDM Past and Present

Since its inception in 2012, the CDM program has evolved to meet the priorities and relative maturity of the FCEB cybersecurity risk posture. When the CDM program began, it focused on implementing a standard set of commercial solutions to meet CDM-identified technical capabilities for enterprise visibility and protection. At that time, the program implemented cybersecurity risk management across the FCEB enterprise. Over time, however, the program recognized the need for flexibility to accommodate unique requirements and differing maturity levels from one agency to the next. Through CDM DEFEND, CISA addressed that need, and built a model focused on long term, sustained engagement, delivering custom solutions tailored to each agency's unique environments and cybersecurity needs.

Within the DEFEND model, CISA has further refined its approach to delivering cybersecurity services. For example, CDM DEFEND activities initially focused on delivering a single capability (e.g. Asset Management or Identity and Access Management) to all participating agencies. After deploying these foundational capabilities, CISA evolved to deliver services based on agency readiness model. In advance of agency engagement, CISA works with the agency to identify where program priorities align with an agency's ability to implement and maintain a specific capability. Using this readiness model, CISA validates that both CISA and the agencies are adequately funded and have the resources necessary to successfully deploy, operate, and maintain the cybersecurity solutions.

The evolution of the CDM program is also driven by new regulations and executive guidance. For example, Executive Order 14028 "Improving the Nation's Cybersecurity" (the "EO"), issued on May 12, 2021, provides greater visibility to agency environments as it grants CISA access to object level cybersecurity data collected through CDM (*see* Section 7(f)). The EO also authorizes CISA to engage in cyber hunt, detection, and response activities through Endpoint Detection and Response ("EDR") solutions deployed through CDM. These EO requirements grant CISA unprecedented visibility into agency network environments to proactively identify and remediate threats and apply observations in one agency environment across the FCEB enterprise.

Through the CDM program, CISA has gained critical visibility into the cybersecurity posture across the entire FCEB enterprise and is well-positioned to quickly identify, assess, and remediate potential threats to agency network environments and, by extension, U.S. national security. Specific accomplishments include the broad roll-out of EDR to FCEB agencies and the onboarding of roughly 250 CISA threat hunters to conduct analysis through EDR and CDM

Dashboard Ecosystem solutions. That access coupled with the availability of object level data through the Dashboard Ecosystem has been a "force multiplier" in providing CISA the ability to identify, assess, and remediate anomalies across the Federal enterprise network.

Future of CDM

CISA continues to evolve its CDM program to meet the needs of its stakeholders. Further, as CISA prepares for the next generation of CDM, it has actively engaged with industry and identified likely future priorities that include:

- Issuing Task Orders based on CDM capability to be applied across the entire FCEB community to promote consistency in solutions across agencies.
- Delivering CDM capabilities to State, Local, Tribal, Territorial (SLTT), and Critical Infrastructure (CI) stakeholders.
- Expanding access to Shared Services across CDM capabilities.
- Enhancing alignment and collaboration among CISA, FCEB agencies, and the cybersecurity tool vendor community.

Concluding Observations

As a federal contractor proudly supporting the CDM program, CGI Federal offers the following observations for consideration:

- Success of CDM's mission depends heavily on FCEB agencies applying the resources and funding to invest in cyber preparedness. Further, funding lapses or delays due to government shutdowns or Continuing Resolutions impact program continuity and ability to operate sustainably.
- Executive Order 14028 "Improving the Nation's Cybersecurity" enhanced CISA's ability to effectively perform its mission through, for example, authorizing CISA to engage in cyber hunt, detection, and response activities through EDR solutions deployed via CDM. Congress could ensure stability in CISA's authority to perform these critical activities by codifying these authorities into law.
- CISA could enable SLTT and CI stakeholders to leverage existing CDM shared service platforms and capabilities to defend against cyber threats such as ransomware attacks. These strategies would allow stakeholders to leverage valuable capabilities in a cost-efficient way to defend against threats such as ransomware attacks.
- The use of the Dashboard Ecosystem and EDR as a "first venue of consultation" for newly identified critical vulnerabilities or anomalous network activity by CISA represents a force multiplier and a new era of centralized hunt and response capabilities within the FCEB. These foundational capabilities can be further leveraged in innovative ways to improve our national security risk posture.

CGI Federal appreciates the critical nature of the CDM program, as well as CISA's core mission. CGI Federal is proud to support CISA and the CDM program in working to secure the federal government's networks for citizens across the United States. CGI Federal also thanks the Subcommittee for its continued oversight to ensure the continued success of the CDM program.