TESTIMONY OF

GREGG T. MOSSBURG

SENIOR VICE PRESIDENT FOR STRATEGIC OPERATIONS

CGI FEDERAL INC.

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY

"CDM: The Future of Cybersecurity?"

January 17, 2018

Good afternoon, Chairman Ratcliffe, Ranking Member Richmond, and other distinguished members of the Subcommittee on Cybersecurity and Infrastructure Protection. My name is Gregg Mossburg. I am the Senior Vice President for Strategic Operations for CGI Federal Inc. ("CGI Federal").

CGI Federal, a wholly-owned U.S. operating subsidiary of CGI Group Inc., is dedicated to partnering with federal agencies to provide solutions for defense, civilian, healthcare, and intelligence missions. Founded in 1976, CGI Group Inc. is the fifth largest independent information technology and business process services firm in the world. CGI Group Inc.'s approximately 71,000 professionals serve thousands of global clients from offices and delivery centers around the world, leveraging a comprehensive portfolio of services including high-end business and IT consulting, systems integration, application development and maintenance, and infrastructure management, as well as 150 Intellectual Property-based services and solutions.

On behalf of CGI Federal's 6,000-plus dedicated employees providing services to over 100 departments and agencies across the federal government, I appreciate the opportunity to testify before the Subcommittee on the progress being made to better secure the federal government's systems through Continuous Diagnostics and Mitigation – otherwise known as CDM.

CGI Federal plays an important role in the CDM initiative, providing credential management ("CREDMGMT") to users at all 23 Chief Financial Officer ("CFO") Act agencies and 3 other agencies to enable greater network visibility. In the next few minutes, I would like to elaborate on the CDM program in general and some of the key factors that have led to very positive collaboration and progress among CGI Federal and its various federal agency clients.

CDM: Risk-based, Cost-effective Cybersecurity across the Federal Government

As you know, cyber threats are growing and evolving continuously. While it is not possible to eliminate or even block all cyber threats, it is critical that the federal government and its contractors focus on identifying security risks, allowing leaders to allocate resources where they will have the greatest impact. To this end, Congress established the CDM program to provide risk-based, cost-effective cybersecurity across the federal government.

The U.S. Government operates some of the largest and most critical networks in the country. As a result, providing security to any one network is a challenge and scaling across the entire federal environment is even more daunting. Consequently, DHS is using an incremental CDM approach to identify and deploy capabilities to participating federal agencies.

The Four-Phase Rollout

The first phase of the CDM program began in January 2013. CDM Phase 1 examined ***what is on the network***. Through discovery tools, a federal agency can identify all of its hardware and software. Using policies and rules, a determination can be made about whether an asset ***should*** be on the network. If it ***shouldn't*** be on the network, then it can be removed. If it ***should*** be on the network, then CDM tools can be used to install patches, continuously scan for vulnerabilities, and ensure that software is configured properly and securely.

While it may not sound as glamorous as penetration testing and cyber threat hunting, studies have shown that cyber hygiene, which consists of four essential activities – *i.e.*, effective asset management, scanning, patching, and proper configuration controls – can stop up to 85 percent of cyber attacks. At the completion of Phase 1, every device in the federal government will have a Master Device Record, allowing increased visibility into these activities.

In June 2016, DHS began rolling out CDM Phase 2. Phase 2 focuses on ***who is on the network***. This phase applies the same concept of "cyber hygiene" to users and helps measure how well agencies comply with existing federal mandates such as the Federal Information System Management Act ("FISMA") and the Homeland Security Presidential Directive ("HSPD") 12. The Phase 2 solutions collect and aggregate information about users from multiple systems into a central location from which agencies are able to monitor different aspects about the users on their respective networks. The centralized Master User Record ("MUR") provides information about individual users to include the degree of vetting, training completed, and credentials issued. This data is important because research continues to show that many security breaches are linked to improper use of credentials (including access through accounts that should have been terminated). Not only will the information collected through the CREDMGMT system allow agencies to understand who is on their network, but it will permit federal agencies to verify that only authorized users with the proper credentials are accessing their networks.

Soon, DHS will be rolling out Phase 3 of the CDM program. Phase 3 is focused on ***what is happening on the network*** and looks to protect the network by monitoring traffic across the boundary and performing software code inspection, application weakness detection, development, and supply chain risk management. Phase 3 also seeks to help agencies manage

security events by preparing for and responding to security incidents using a new automated risk assessment process to replace the current manual, time-intensive process.

The requirements for CDM Phase 4 are still evolving, but DHS has indicated that it will focus on ***how data is protected*** through technologies such as micro-segmentation, digital rights management, and other advanced data protections.

Data from all phases of the CDM program is channeled to agency-level dashboards for display and action. Information from these agency dashboards is aggregated into a federal-level dashboard to provide a government-wide view of how agencies are performing and identify the greatest areas of risk for corrective action. This data also can be analyzed and presented in meaningful ways to various consumers and decision makers such as senior leaders interested in trend analysis and technical experts looking to take a deep dive into the detailed technical information.

Deployment across Agencies

Not only is DHS incrementally rolling out cyber capabilities, it has taken a staggered approach to deploying those capabilities to all federal agencies. In Phase 1, agencies were divided into buying groups of 5-7 agencies (Groups A, B, C, D, E, and F) with a single integrator responsible for deploying a solution to agencies in each group, typically over a 3-year period. For Phase 2, DHS issued two (2) task orders each with a 2-year duration. The first task order addresses privileged users (*i.e.*, users with extra power or control over the computer system who have the ability to do the most harm) at 65 federal agencies. This task order effort is commonly referred to as the privilege management (or "PRIVMGMT") task order. The second task order – which CGI Federal currently is delivering – is CREDMGMT, which has a 2-year duration and covers all users at 23 CFO Act and 3 other agencies.

The CDM program often is discussed in the context of tool acquisition. Yet, the integration and consulting services provided are key to federal agency success. Given the shortage of cybersecurity professionals, the vast number of security products available, and competing IT priorities, federal agencies often are in need of cyber security experts and skilled IT resources. The CDM program recognizes these needs and provides not only cyber expertise, but also services for training, testing, and governance to help agencies develop processes and policies.

A New CDM Acquisition Strategy

As with all programs of this size, there are trade-offs to be considered. For example:

- the economies of scale and repeatability of using a consistent solution across the federal government versus tailoring to a specific agency's existing infrastructure and processes;
- using a single integrator with deep expertise in a solution across a large number of agencies may speed overall deployment, but delay agency-specific process changes; and
- a single integrator supporting an agency for a long period of time will have a deep understanding of the agency's environment, but may not have the required expertise in all cyber products.

As a result, DHS and GSA-FEDSIM carefully evaluated these trade-offs with the lessons learned on the original CDM contract and addressed them in the new series of CDM acquisitions, called Dynamic and Evolving Federal Enterprise Network Defense (or "DEFEND").

Some of the benefits of the new DEFEND strategy include:

- Providing a longer period of performance to encourage a strategic partnership between the integrator, agency, and DHS while helping to address the challenge of processing background investigations for multiple integrators;
- Creating a separate acquisition process for tools and implementing a CDM Approved Products List ("APL") to remove the tool vendors' dependency on integrators;
- Providing flexible funding scenarios, such as incremental funding, allowing agencies to jointly-fund efforts with DHS, and surge options; and
- Providing agencies at different levels of maturity with the flexibility to address their most pressing needs.

A Collaborative Partnership

As noted earlier, CGI Federal currently is delivering the CREDMGMT solution to 26 agencies under a 2-year task order. To date, this complicated IT implementation effort has enjoyed remarkable collaboration among CGI Federal, the agencies, and DHS (supported by GSA-FEDSIM), allowing the team to make great progress. In fact, early deployments already have provided agencies with insight into potential issues that now can be addressed.

An Impressive Undertaking

While everyone feels the urgency brought on by continuous cyber-attacks, it is important to not lose sight of the fact that providing security to networks as large and complex as those of the U.S. Government is an enormous undertaking. This is one of the first efforts of its type, therefore, it is critical to lay a solid foundation on these programs before building more advanced capabilities.

CGI Federal is proud to support the CDM program and help its federal agency clients protect our country's networks, assets, and information. CGI Federal relishes this rare opportunity to work across the entire federal government to identify trends and connect agencies to share best practices and lessons learned.

Let me close first by thanking the folks at DHS, and particularly the National Protection and Programs Directorate, for their partnership and urgency in supporting the CDM implementation. It would be an understatement to say that DHS is responsible for overcoming numerous critical challenges in the protection of our country every day. CGI Federal respects DHS' focus on schedules, budgets, and its relentless drive to get the best from industry. I also want to thank this Subcommittee for its continued oversight to ensure the continued success of the CDM program. Mr. Chairman, I look forward to answering any questions that you or the Subcommittee may have.