TESTIMONY of

Stephen (Max) Everett
Chief Information Officer
U.S. Department of Energy

Before the

Subcommittee on Cybersecurity and Infrastructure Protection of the
Committee on Homeland Security
and
Subcommittee on Information Technology of the Committee on Oversight and Government Reform
U.S. House of Representatives

March 20, 2018

* * *

Good afternoon Chairmen Hurd and Ratcliffe, Ranking Members Connolly and Richmond, and distinguished Members of the Committees. On behalf of the Secretary and Deputy Secretary of Energy, I thank you for inviting me to testify about the Department of Energy's (DOE or Department) experience with Continuous Diagnostics and Mitigation (CDM) capabilities and tools.

DOE PRIORITIES

As the Department's Chief Information Officer (CIO), I report directly to the Secretary and Deputy Secretary, properly positioning me to ensure that decision-making processes across the Department factor in Information Technology (IT) and cybersecurity considerations from the outset. The Secretary and Deputy Secretary have repeatedly emphasized to senior Departmental leadership the importance of weaving cybersecurity into the fabric of DOE policy and operations. They understand that the first step toward protecting information and systems is to have visibility into what is connected to and runs on DOE networks.

Chairman Hurd, at the Federal Information Technology Acquisition Reform Act (FITARA) 5.0 hearing this past November, you asked me whether I could say that I knew everything that was connected to DOE networks. My response then was blunt: I said I could not. Today, four months later, while that message has not changed, I am pleased to talk about the work we are doing to be able to answer that question with an emphatic "yes." The lack of fidelity and visibility about what is connected to DOE's networks raises our cybersecurity risk profile to an unacceptable level; urgent action is needed.

The Secretary and Deputy Secretary are aware of this issue and fully support our enterprise-wide plan of action to obtain fidelity and visibility, enabling DOE to properly protect its networks. We know that CDM tools and capabilities are essential to providing visibility into the content and

connectivity of our networks. That is why the Secretary and Deputy Secretary have given me clear direction to implement CDM as swiftly as possible where gaps exist across the DOE enterprise, including at the National Nuclear Security Administration (NNSA) and its National Laboratories, the Office of Science National Laboratories, the Power Marketing Administrations, plants, and sites. We also recognize that CDM capabilities and automated data collection and flow will enhance DOE's Integrated Joint Cybersecurity Coordination Center (iJC3)—which provides cybersecurity threat analysis, tracks advanced persistent threats, and distributes automated threat information—by providing additional visibility into the network enterprise-wide. Furthermore, CDM will accelerate the availability of the more detailed, relevant, and reliable data necessary to better inform our Enterprise Risk Management processes.

Implementation of CDM Phase 1 and 2 has been accomplished for DOE Headquarters. This is approximately 8 percent of the Department's networked endpoints. I am pleased to report that the Department is looking forward to deploying the common elements of the CDM platform across the DOE enterprise to fill gaps in current capabilities. The Department developed a 180-day strategy to identify and address gaps in CDM Phase 1 and 2 capabilities and to plan implemention of Phase 3 capabilities. This, in combination with mutually reinforcing, ongoing IT modernization efforts, will be calibrated to ensure DOE's continued mission success throughout the enterprise.

CDM STATUS

The Department recognizes that sound and comprehensive vulnerability detection requires a multidimensional approach involving asset management, automated tools, monitoring of communication channels, and human analysis. We believe that implementing CDM capabilities will play a key role in this multidimensional effort.

Unfortunately, we are still in "catch-up" mode with implementation of CDM enterprise-wide. The Department took a scaled approach to CDM Phases 1 and 2. Before embarking on the larger-scale deployment of CDM across the DOE enterprise, DOE first piloted tools and sensors on the Energy Information Technology Services (EITS) network, which is the network the Office of the CIO directly manages.

We fully implemented CDM Phase 1 tools and sensors across EITS, and successfully tested data transfers with the Department of Homeland Security (DHS). Further, we procured the tools to implement CDM Phase 2 for EITS and are working with a vendor on that implementation. We estimate completion in November 2018.

CDM NEXT STEPS

While we are taking measured, prioritized actions to meet our goals, we appreciate the cooperation and collaboration of our DHS partners. In partnership with DHS, we will conduct a CDM Phase 3 needs assessment—enterprise-wide—to identify and address gaps for the remainder of the Department, including NNSA and its National Laboratories, the Office of Science National Laboratories, the Power Marketing Administrations, plants, and sites. I am

pleased to report that we have a high level of confidence in our gap analysis methodology, cost estimates, and due diligence.

In the coming weeks, we intend to utilize the CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) Request for Service (RFS) Process to address Phase 1 and 2 gaps in deployment in addition to Phase 3 and 4 Planning and Implementation requirements. We have incorporated lessons learned from our EITS pilot to streamline the Department's approach and planning as we progress through CDM Phases 3 & 4 with DHS.

My assessment is that CDM capabilities will complement and enhance DOE's IT modernization efforts by helping us identify and prioritize legacy systems in need of remediation. OCIO recognizes that it is not prudent to apply CDM to failing network infrastructures or outdated systems that use legacy software, some of which are no longer supported. While this change will be uncomfortable at first, streamlined and prioritized IT modernization efforts that are fully-informed by CDM will, in turn, lay a foundation for further security upgrades, including the components of CDM Phases 3 and 4, and should result in better network security and cost savings through operating efficiencies.

OPPORTUNITIES FOR IMPROVING CDM

Opportunities exist for additional streamlining and acceleration of the CDM implementation process. We will make the most progress when we lead with the areas where shared platforms hold the most obvious and direct opportunities for improved visibility, awareness, and ongoing mutual benefits between DOE and federal agencies. On the other hand, where we have exceptions that require special considerations due to unique environments and mission requirements, we are committed to finding ways to account for their presence on the network, as well as identifying opportunities to adapt or upgrade those systems to make them compatible with enterprise-wide CDM.

We encourage DHS to continue to work actively and collaboratively with their counterpart departments and agencies to develop the CDM dashboard and associated metrics, which need to be usable and actionable by providing relevant threat and vulnerability information. I am confident that the CDM dashboard will provide significant value to the Department as CDM is implemented across the enterprise. The value of the CDM dashboard will be the extent to which it allows us visibility into the networks while providing actionable information and intelligence that can drive real-time decisions that result in increased protection for DOE systems and information. Establishing a credible feedback loop that takes into account the customers' requirements across the federal enterprise is essential.

We also encourage DHS to continue to actively work with DOE and other departments and agencies in the decision-making processes around the maturation of the CDM program, particularly with regard to contracts, metrics, priority data, and parameters. To have a truly shared platform, we need the information to flow in both directions. Collaboration and cooperation are key to mission success government-wide. Having a genuine shared platform means having a shared responsibility for the information that we feed into the system, as well as for the information we will receive and use for threat analysis and incident response.

WORKFORCE

At DOE, our people are the key to and foundation of our mission success. We are focused on developing our employees' expertise, expanding our talent pool, and working to optimize the integration of automated systems, such as CDM, to find ways for systems to conduct the automated tasks and large-scale processing for which they are best suited.

Further, we must attract and retain a world-class cybersecurity workforce that has the skills necessary to successfully broker and oversee cloud and managed-services solutions, and make key decisions about how best to use new and rapidly-changing information both tactically and strategically.

CDM AND DIGITAL TRANSFORMATION

In addition to implementing CDM, DOE is conducting a range of IT modernization efforts that are mutually-reinforcing with CDM's enhancements to network security. As we continue to implement CDM, it will generate data and visibility that will accelerate these modernization efforts, and the modernization projects will, in turn, provide a robust infrastructure for the deployment of additional tools and capabilities, including CDM.

DOE is currently developing a Digital Transformation Strategy (Strategy), which will provide an enterprise plan of action and include a mechanism to measure results through enterprise requirements for the Department. In addition, we are developing an Enterprise Architecture and Roadmap tied to our Strategy.

Our Strategy will be built on a "Cloud First" policy to transition from service owner to service broker. Consistent with the President's direction in the IT Modernization Report, the Cloud First policy fosters innovation, reduces costs, improves interoperability, scales capacity to match demand, lowers operational costs, and establishes the bedrock for future enterprise capabilities.

We have initiated seven Digital Transformation Work Streams to define enterprise requirements and develop further recommendations for modernization. These are: Trusted Internet Connection, Collaboration Tools and Services, Directory Services, Data Center Optimization, Email, Network Transport, and Mobility.

The Department's Data Center Optimization Work Stream is expected to identify multiple opportunities for IT Modernization from consolidation, virtualization, and cloud migration. Our goal is to move IT workloads to the cloud, maximize virtualization, meet data center closure targets, and retrofit the remaining data centers for optimal energy efficiency while reducing costs.

We also have efforts underway to modernize DOE Headquarters networks to a level consistent with the capacity, agility, and resiliency of modern enterprise networks. This will establish the base for commercial/managed-service implementations of services with engineered and inherent cybersecurity capabilities, such as Infrastructure-as-a-Service and Platform-as-a-Service in

support of the Data Center Optimization Initiative, and Enterprise Software-as-a-Service solutions like cloud email and Desktop-as-a-Service, while providing foundational requirements for enhanced cybersecurity tools, products, and capabilities.

CONCLUSION

Enterprise-wide CDM is a high priority for DOE, because of the range of benefits we expect to see from its full implementation. CDM will assist us with other critical and long-overdue efforts, such as IT Modernization, while also providing us with timely, actionable information to help us secure DOE information and systems.

I appreciate the Committees' interest in this important topic, and I look forward to continuing to work with our partners in Congress, as well as our colleagues at DHS and across the federal government, to achieve our shared goals. It has been my distinct honor to testify before you today, and I would be pleased to address your questions.