Statement for the Record

of

Kevin Cox
CDM Program Manager, Network Security Deployment,
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
U.S. House of Representatives
Subcommittee on Cybersecurity and Infrastructure Protection
Committee on Homeland Security

and

Subcommittee on Information Technology
Committee on Oversight and Government Reform

Regarding

Continuous Diagnostics and Mitigation

March 20, 2018

Chairman Ratcliffe, Chairman Hurd, Ranking Member Richmond, Ranking Member Kelly, and members of the Subcommittees, thank you for today's opportunity to discuss the state of federal cybersecurity. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. This past December, the House voted favorably on H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." If enacted, this bill would mature and streamline NPPD, renaming our organization as the Cybersecurity and Infrastructure Security Agency to clearly reflect our essential mission and role in securing cyberspace. The Department strongly supports this much-needed legislation and encourages swift action by Congress to complete its work on this legislation.

NPPD is responsible for collaborating with federal agencies to protect civilian federal government networks, as well as with the Intelligence Community; law enforcement; state, local, tribal, and territorial governments; and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to protect their cyber systems and quickly recover should such an incident occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing on best practices and cyber threats, and strengthen resilience.

Cybersecurity Priorities

This Administration has prioritized protecting and defending our public and economic safety from the range of threats that exist today, including those emanating from cyberspace. Last year, the President signed Executive Order (EO) 13800, on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. This order also emphasized the importance of accountability – clarifying that agency heads are responsible and will be held accountable for the security of their networks and systems. NPPD plays an important role in providing capabilities, services and direction to federal agencies.

Although federal agencies have primary responsibility for their own cybersecurity, DHS, pursuant to its various authorities, provides a common set of security tools across the civilian executive branch and helps agencies manage their cyber risk. NPPD's assistance to federal agencies includes:

- providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN", and the Continuous Diagnostics and Mitigation (CDM) programs;
- measuring and motivating agencies to implement policies, directives, standards, and guidelines;
- serving as a hub for information sharing and incident reporting; and

- providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services.

Today, my testimony will focus on one of the capabilities NPPD has to assist federal agencies with their cybersecurity and DHS with protecting the federal enterprise—the Continuous Diagnostics and Mitigation (CDM) program. CDM provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common federal dashboard.

In the first phase of CDM, the National Protection and Programs Directorate (NPPD) is helping federal agencies better understand what is on their network and better manage the cybersecurity of those assets. CDM works to ensure that agencies know what IT assets they operate and how well those assets are configured and patched. IT assets, combined with their vulnerabilities and misconfigurations, represent a significant attack surface that our adversaries target. Through better patching and configuration, agencies are able to reduce the likelihood of successful compromise against the evolving threat. This is one of the key objectives of CDM.

Another fundamental principle of CDM is to understand who is on the network, which we address through Phase 2. By learning who has access to agency networks, including those individuals with privileged user access, agencies can appropriately restrict network access and ensure the principle of least privilege is being followed. This second phase of CDM is a significant step forward in managing cyber risk.

CDM is helping us achieve three major advances for federal cybersecurity.

First, agencies are gaining continuous visibility, often for the first time, into the extent of cybersecurity risks across their entire network. With enhanced visibility, they can prioritize the mitigation of identified issues based upon their relative importance.

Second, with the federal dashboard, the NCCIC will be able to operationalize this visibility, initially through improved vulnerability management. For example, the NCCIC currently tracks government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will transform this, enabling the NCCIC to immediately view the prevalence of a given software product or vulnerability across the Federal Government so that the NCCIC can provide agencies with timely guidance on their risk exposure and recommended mitigation steps.

Third, through the CDM program, the DHS is building important partnerships with the General Services Administration (GSA), other federal agencies, and industry to directly address the nation-state and criminal threats against our critical data and federal networks.

Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian executive branch.

Moving forward, the new CDM DEFEND Acquisition Strategy, developed in partnership with GSA, incorporates lessons learned from the Continuous Monitoring as a Service Blanket Purchase Agreements that were used in the early stages of the CDM Program. CDM DEFEND contracts have longer periods of performance with higher contract ceilings providing agencies more flexibility. This flexibility will allow agencies to modernize and standardize their security capabilities in a way that meets the CDM requirements and makes the most sense for each organization. CDM DEFEND will also support legacy and new infrastructure requirements such as cloud and mobile and will allow agencies to procure cybersecurity tools and services separately or together.

Conclusion

In the face of increasingly sophisticated threats, NPPD supports the Federal Government's efforts to defend our Nation's federal networks and critical infrastructure from cyber threats. Our information technology is increasingly complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "Internet of Things" (IoT) and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our Nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

Thank you for the opportunity to testify, and I look forward to any questions you may have.