UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

TESTIMONY OF
DAVID GARCIA
CHIEF INFORMATION OFFICER
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the
SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION
COMMITTEE ON HOMELAND SECURITY
AND
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

"CDM: Government Perspectives on Security and Modernization"

March 20, 2018

Thank you Chairman Ratcliffe, Chairman Hurd, Ranking Member Richmond, Ranking Member Kelly, and Members of the Subcommittees for engaging in this important discussion. I appreciate the opportunity to appear before you today.

Although I am new to the U.S. Office of Personnel Management (OPM), having only been at the agency for about six months, I am pleased with the transformative activities that my office has already undertaken. Since arriving, I have worked with senior staff to identify key priorities to drive our efforts and to build governance processes to support our work. We recognize that OPM is an organization made up of terrific people with a mission to serve not just the Federal workforce, but also the American people. To successfully meet this important mission, OPM will continue to bring to the Federal government agile, modern Information Technology (IT) solutions that reflect its needs and leverage forward-leaning capabilities. The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Program is an important element to assist us with this goal.

As the former Chief Information Officer (CIO) for the State of Maryland, and with over 20 years of private sector executive experience, I look at OPM's current posture through both a private and public sector viewpoint. There are two main points that I think are critical to the context of the conversation we are having today regarding CDM. First, we must understand that CDM is a

broad approach and is continuously evolving. Every day the malicious actors around the globe, who are equivalent to military grade adversaries, are adapting. Therefore, as Federal agencies, we need to have the flexibility to adapt. Second, we must strive to have CDM and similar future programs, reduce the time required for the public sector to procure technological solutions compared to the time it takes in the private sector, which contributes to a gap in preparedness. As an entrepreneur and small business owner in the private sector, I had the flexibility to procure and implement a solution to mitigate a zero-day threat or vulnerability immediately; however, as the CIO for a Federal agency, I do not have that same flexibility to get needed tools on our network in real-time. While CDM has certainly reduced the procurement timeframe for cybersecurity technology, a goal should be to continue to enhance the ability for agencies to procure what they need to maintain the appropriate cyber defenses as quickly as possible. The faster agencies can procure technology, the faster technology can be implemented – which gives agencies the best chance to stay ahead of possible threats that continue to evolve and become more sophisticated.

Since coming to OPM, I have developed a vision of the top five priorities the CIO must address to successfully support OPM. Those priorities are: 1) continue to fully mature the Risk Management Program by building on OPM's cybersecurity success to date, applying new technologies and techniques, and implementing the best practice recommendations from the Department of Homeland Security, the Government Accountability Office, and OPM's Inspector General, as appropriate; 2) work with stakeholders to provide new and innovative customer experiences through the latest technology; 3) utilize technology to reduce the investigation inventory; 4) create IT financial transparency through implementation of a standardized technology with the ability to develop a sustainable, transparent, and repeatable financial model; and 5) align the CIO organization to better meet the needs of OPM by providing a foundation for current and efficient services that will last longer than the lifespan of a server and that can be leveraged for the long term.

CDM supports these priorities and OPM will continue to build off of its successful implementation of CDM's Phase 1 and the continued implementation of Phase 2. As you may know, OPM is one of the first agencies to fully implement CDM, and we have benefited from the enhanced visibility into who and what is on our network so that we can more accurately and rapidly respond to potential risks. OPM completed implementation of CDM Phase 1 with the CDM dashboard fully populated in the spring of 2017 using the CDM sensors we've been deploying since 2015. This phase focuses on managing "what is on the network," to include the management and control of devices, software, security configuration settings, and software vulnerabilities. For OPM, this has meant gaining greater insights into connection points within our network, which provides us with the ability to better regulate devices connecting to the environment as well as a better understanding of what should actually be on the network. In addition, OPM made use of CDM technologies to identify and strategically resolve potential vulnerabilities, which has resulted in better overall risk management and response.

OPM is on track to complete implementation of CDM Phase 2 in the summer of 2018, ahead of the scheduled fall 2018 target for the Federal government. Phase 2 focuses on the management and control of user access privileges. Phase 2 has allowed OPM to standardize the access of systems so that the management of all accounts is unified and controlled through an agency governance process. Reducing the volume and scope of user access also helps OPM identify anomalies related to possible insider threat activities and prevent data loss. Access for privileged users, which are users that have some administrative access to systems or data, is being enforced through a separate login mechanism. Our next step toward completion of CDM Phase 2 is to activate additional two-factor authentication enforcement features. This is especially critical in the context of the events of 2015 because it will add additional two-factor authentication requirements to address longstanding audit findings.

OPM has been successful in the implementation of Phase 1 and 2 of CDM due to the alignment of the technology available through CDM with agency technology strategy and life cycle management. The use of CDM has set the stage for OPM to move into a Continuous Monitoring approach that enhances OPM's ability to manage its systems and continually evolve to secure its systems in near real-time.

I am also pleased with how CDM Phase 3 has evolved from offering very specific software or capabilities within certain National Institute of Standards and Technology control families to a "buffet" style offering with software and capabilities supporting the necessary agility that Federal agencies require to meet the unique needs and goals related to their specific operations. Looking forward, OPM will increasingly leverage CDM for our procurement needs to meet new challenges. We will prioritize our risk management needs and align the new technologies offered by CDM to meet our highest risks in a continuous effort to reduce vulnerabilities.

I see Phase 4 of CDM transitioning into an ongoing and continuous monitoring effort that will allow OPM and other agencies to keep pace with malicious actors. For agencies to be successful, Phase 4 should allow the Federal government the ability to move as quickly as new technologies and threats evolve. This can be accomplished through an offering of tools and services that meet the specific goals and needs of agencies and through agile procurement capabilities that allow agencies to change and adapt their tools in real-time. Following best practices in government procurement, coupled with a continued effort to survey what capabilities are available throughout the private sector, will help keep the Federal government informed and on pace. For CDM to be successful in the long term, it will need to continue to evolve, including the use of new ideas and concepts, such as the use of Artificial Intelligence (AI), for immediate identification, response, and updates to threats. Due to the asymmetric nature of attacks, we also need to consider security risks related to the increasing use of AI by our adversaries across all sectors and how that may impact the kinds of cyber defense and tools we need.

I accepted the position of CIO at OPM because I truly believe in the OPM mission and because it is an agency in which great success can be achieved and demonstrated. The people at OPM are

dedicated, new technology is being implemented, and the agency is committed to supporting all the Federal employees who devote their lives to serving the American people. Although there may be bumps in the Federal government's journey to keep pace with potential cyber threats, I am confident we have an incredible opportunity to make strides towards a successful future. I look forward to working with the Members of these Subcommittees to continue our efforts of IT modernization and the evolution of the CDM Program so that it will remain a successful resource for Federal agencies.

Thank you for the opportunity to testify before you today. I look forward to answering any questions you may have.