IT Alliance for Public Sector
A Division of ITI

Oral Testimony of

A.R. "Trey" Hodgkins, III

Senior Vice President

IT Alliance for Public Sector

Before the

U.S. House of Representatives Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure Security

January 17, 2018

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Committee, on behalf of the members of the IT Alliance for Public Sector, or ITAPS, thank you for the opportunity to share our perspectives today on the Department of Homeland Security Continuous Diagnostics and Mitigation program. ITAPS represents almost 90 of the most innovative companies offering IT goods and services in the federal public sector. We applaud the Committee's efforts to understand and explore the CDM program, the state of CDM tool acquisition, and what barriers in policy or practice exist to rolling out CDM across the federal government.

Last year, ITAPS provided the Administration with numerous recommendations to modernize federal cybersecurity practices, including how to protect federal networks through accelerated adoption of Einstein and the CDM program. These recommendations include: requiring regular, automated, vulnerability scanning of federal networks; updating procurement guidance to reflect the speed of cyber threats; expanding existing programs to recruit and retain a strong cybersecurity workforce; and, leveraging new technology and integrating security tools into IT deployments.

DHS is implementing recommendations included in the President's IT modernization report. These range from

securing government systems in commercial clouds - something not included in the original CDM plan - to completing the acquisition strategy for new, long-term task orders that offer CDM lifecycle support to agencies. ITAPS suggest that Congress focus on the following:

1. **Accelerate procurement cycles to keep pace with cyber threats.** The committee should work to ensure that there are sufficient numbers of adequately trained contracting personnel to deploy CDM tools in a timely fashion to keep up with the evolving threat landscape.

2. **Accelerate the Adoption of CDM through oversight.** The committee should exercise oversight to ensure that

agencies are prioritizing funding for CDM solutions because agencies are reluctant to contribute to funding their own security. Many don't put a line item in their budget requests and seek to rely solely upon DHS funding for CDM deployment. Unpredictable federal appropriations substantially contribute to this condition, as agencies are not able to effectively plan, identify, acquire, and deploy cyber tools in truncated budget cycles.

3. **Experienced personnel with the appropriate skillsets and vendors with proven success at enterprise scale are critical to the success of CDM.** The committee should work with DHS to ensure that the acquisition

plan for Phase 3 contemplates the skills necessary for effective implementation, the budget to attract and retain individuals with such skills, and vendor qualifications based on experienced success.

4. **Protect federal data.** It has been almost 3 years since the OPM data breach and DHS has yet to implement Phase 4 of CDM to provide data level protection capabilities, such as digital rights management, micro-segmentation, and data masking.

5. **Enhance accountability for agency adoption and deployment of CDM through robust use of the CDM dashboard.** The federal dashboard compiles summary feeds from all the agencies regarding their adoption and

deployment of CDM. This tool will eventually provide a broad view of the government's cyber posture to help DHS and OMB determine where resources are needed to strengthen agency systems. The CDM dashboard is also one specific means for Congress to hold agencies accountable for their progress.

6. **The CDM Program Office should educate state, local and tribal governments about the CDM tools and capabilities available.** State,local and tribal governments are facing similar cyber challenges and threats and governors have made cybersecurity a top priority. But many need help with protecting their data and networks. The committee should work with DHS to

create an outreach program to ensure that these other government jurisdicitions are aware of CDM, the tools and capabilities that are available and how they can acquire CDM capabilities for their own use through Schedule 70 at GSA.

7. **Ensure adequate means to attract and retain a cyber-skilled workforce.** Congress should create innovative means to attract cyber-skilled applicants and retain them once hired. It should also look to rapidly draw down the security clearance backlog. Imagine what the government cyber workforce could do if just ten percent of the over seven hundred thousand employees and contractors awaiting investigations could get cleared?

To close, the technology sector supports the CDM program and its' various phases as an important and effective means to securing the federal government networks and systems. More improvements can be made, though, and I hope that our recommendations can help the committee focus on making CDM better.

We look forward to the opportunity to work with Congress and the Department on this important issue. I am happy to answer your questions at the appropriate time and thank you again for the opportunity to share our perspectives.