Opening Statement of Ranking Member Cedric Richmond

Subcommittee on Cybersecurity and Infrastructure Protection Joint Hearing

CDM: Government Perspectives on Security and Modernization

Tuesday, March 20, 2018

The Continuous Diagnostics and Mitigation (CDM) program is a key component of the Department of Homeland Security's (DHS) overall effort to protect the ".gov" domain. Through CDM, DHS works with agencies to procure cybersecurity tools and services that will enable them to identify and defend against attacks. These tools are increasingly important in today's security environment.

Every year, Federal networks get hit by tens of thousands of attempted intrusions – many of them highly-sophisticated, state-sponsored attacks. According to the Office of Management and Budget, Federal agencies endured over 35,000 cybersecurity incidents in Fiscal Year 2017, which is higher than previous years. As initially envisioned, CDM would provide Federal agencies with the information and tools necessary to protect their networks, including:

- What devices and assets are on an agency's network?
- Who has access to an agency's network, including those parts of the network reserved for privileged users? *and*
- What happens on the network, and how data is stored and protected?

Unfortunately, agencies have been slow to realize the potential benefits of CDM due to unanticipated implementation challenges. For example, Federal agencies struggled to complete the difficult task of identifying all of the devices, assets, and endpoints on agency networks. Moreover, when the Cybersecurity and Infrastructure Protection Subcommittee held a hearing with CDM contractors in January, witnesses observed that many agencies lack personnel with the appropriate training and expertise to reap the full value of CDM tools, particularly the dashboards.

This Subcommittee has repeatedly examined cyber workforce challenges throughout the Federal government, and our witnesses in January reminded us that there is no silver bullet technology can replace human capital. We also learned that, although the CDM program has been in place for five years, agencies still do not have full visibility into the IT assets on their networks. Without this visibility, it is impossible for agencies to know *who* has access to their networks, and *what* exactly they need to protect. Today's witnesses can provide an important and informed picture of how CDM tools and services are being adopted and deployed at their respective agencies.

I am interested in knowing not only the status of implementation, but also how these agencies are working with the Department of Homeland Security, and how effectively the Department has been able to respond to agency needs. I also hope to hear what Congress can do to make sure CDM is an effective tool for raising the bar on cybersecurity throughout the Federal government.

Last week, the Department of Homeland Security and the FBI issued a technical alert on the Russian government's efforts to use cyber tools to target U.S. government entities. These cyberattacks were carried out over the course of 2016, and parallel Russia's attacks on our electoral system and democratic institutions.
It is clear that the Kremlin will continue to be relentless in its assault on our Federal networks, and the networks that support our nation's critical infrastructure. And, we know that China, Iran, and North Korea are sophisticated cyber actors that are constantly working to build a more robust cyber "arsenal" that could be used against our Federal networks. We must remain vigilant in protecting the .gov, and do everything in our power to ensure the Federal government has the resources needed to act quickly to protect itself.