Statement of Ranking Member Cedric Richmond (D-LA)

Subcommittee on Cybersecurity and Infrastructure Protection Hearing

CDM, the Future of Federal Cybersecurity?

Wednesday, January 17, 2018

Today, DHS is working to protect Federal networks by administering two signature programs – EINSTEIN and CDM. These programs work in tandem to keep out unauthorized traffic and provide ongoing monitoring and mitigation of cybersecurity risks. Through CDM, the Department works with Federal agencies to procure cybersecurity tools and services to empower them to fend off cyber-attacks.

As initially envisioned, CDM would provide each agency with the information and tools necessary to protect its network by, among other things, identifying the assets on an agency's network that warrant protection, bolstering access controls to various elements of an agency's network, and improving situational awareness about activities on an agencies network.

Implementation of CDM, however, has been slower than DHS anticipated. Challenges inherent to the size and scope of the task of accounting for all assets on the Federal network, confusion about whether DHS or a customer agency was responsible for footing the bill for CDM-related expenses, and technology gaps in the commercial-off-the-shelf markets have collectively slowed the process.

That said, today about 20 agencies have their internal dashboards up and running and two agencies have connected to the Federal dashboard. And by next month, DHS expects that all 24 of its target agencies to be connected to the Federal dashboard.

As more agencies connect to the Federal dashboard, DHS will have greater visibility across Federal networks and will be better-positioned to identify and mitigate malicious activity, including complex, coordinated attacks.

As representatives of vendors who work directly with DHS on CDM, the witnesses here today have a unique perspective on how to ensure Federal agencies continue to prioritize cybersecurity investments, how the Federal government can implement the lessons learned over the past five years to improve the program, and whether contracting personnel have the training necessary to deploy CDM quickly.

I also hope to witnesses can speak to how the Department's failure to name a permanent Under Secretary for the National Protection and Programs Directorate, along with ongoing Chief Information Officer vacancies across the Federal government, are affecting implementation of CDM.

Our adversaries have made their interest in breaching Federal networks clear. Just last week, Trend Micro reported that Fancy Bear, the same Russian-backed hacking group that breached the Democratic National Committee in 2016, has been targeting the Senate's network.

Although Congressional networks do not participate in CDM, this troubling report serves as a reminder that the interest in breaching U.S. government networks persists and that the Federal government must act more quickly to protect itself.

On a final note, this Subcommittee is also responsible for ensuring that Federal policies support private-sector efforts to secure critical infrastructure. Last summer, reports emerged that hackers successfully penetrated domestic energy companies and nuclear power plants.

In light of the growing cyber threats against critical infrastructure, I will be interested in learning whether the private sector can benefit from implementing elements of CDM and whether efforts to implement CDM-like programs are already underway.