COMMITTEE ON HOMELAND SECURITY DEMOCRATS

Rep. Bennie G. Thompson, *Ranking member*

FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson (D-MS)

CDM: Government Perspectives on Security and Modernization

Cybersecurity & Infrastructure Protection Subcommittee Joint Hearing

March 20, 2018

The Continuous Diagnostics and Mitigation (CDM) program is a key part of our national approach to secure Federal networks, which Americans rely on to store some of our most sensitive national data – from health records and Social Security Numbers to the holdings of critical infrastructure owners and operators and national security documents.

Over the past decade, we have seen the number of cyberattacks against Federal agencies rise exponentially. According to the Government Accountability Office cyberattacks have risen by more than 1,000% since 2006.

The Office of Management and Budget reports that Federal agencies endured more than 35,000 cybersecurity incidents last year alone.

Some of the officials testifying on today's panel know all too well how much damage can flow from a high-profile breach.

For instance, the Veterans' Affairs Department reported in 2013 that its databases had been hacked by no less than eight foreign governments.

And in 2015, the Chinese government infiltrated the Office of Personnel Management's systems and accessed the personal information of more than 22 million past and present Federal employees.

Last week, we turned our attention to bold attacks carried out by the Russian government in 2016 to access and gain control of the central command centers that support our electrical grid, nuclear power plants, and our water supply.

Even the Secretary of Energy admitted that he was "not confident" in the ability of the Federal government to counter foreign adversaries in cyber space.

These hackers show no signs of slowing down. Instead, they have only grown more aggressive and more sophisticated.

Federal agencies need robust cybersecurity now more than ever – and CDM has the potential to be an important line of defense.

Through the CDM program, DHS works with Federal agencies to procure cybersecurity tools and services to fend off cyber-attacks.

The program works in tandem with EINSTEIN to keep out unauthorized traffic, continuously monitor for threats, improve visibility of network assets, and prioritize efforts to correct vulnerabilities.

Unfortunately, Federal agencies have been slow to adopt and fully deploy CDM technologies.

In a hearing earlier this year, we learned that agencies and CDM vendors are struggling to compensate for a lack of cyber expertise among agency personnel.

The witnesses told us that these employees need to be better trained on how to use CDM tools in order to reap all the security benefits they provide.

We also heard that, after five years, agencies still do not have a full accounting of all the devices connected to their networks.

Agencies need this visibility, since they cannot protect what they do not know they have.

These obstacles are compounded by the staggering number of cyber vacancies throughout the Federal government, both for rank-and-file civil servants, as well as key leadership positions.

Far too many agencies are still operating without a permanent Chief Information Officer in place.

We need to understand the challenges agencies are facing when it comes to purchasing, installing, and deploying CDM capabilities, and we need to make sure you have the resources, support, and statutory authority necessary to continue moving forward.

# # #

Media contact: Adam Comis at (202) 225-9978