



HOMELAND SECURITY COMMITTEE

Statement of Subcommittee Chairman John Ratcliffe (R-TX) Cybersecurity and Infrastructure Protection Subcommittee

"CDM: Government Perspectives on Security and Modernization"

March 20, 2018

Remarks as Prepared

This is the second hearing this year that the Cybersecurity and Infrastructure Protection Subcommittee has held on the Continuous Diagnostics and Mitigation or CDM program. That is because I see real value in the goals of CDM not only for cybersecurity, but also for improving the efficiency of information technology across the board.

To that end I am pleased to be holding this hearing today jointly with my good friend from Texas, Mr. Hurd – who has been a leader on IT modernization issues as the chairman of the Subcommittee on Information Technology.

We welcome our friends from the Oversight Committee to the CDM conversation.

I believe that DHS' CDM program has great potential to drive progress on a number of cybersecurity issues— from network visibility to data centric security and from the role of increased automation of security tasks to the role of artificial intelligence.

So the question I have to this panel today is – what can we as Congress do to make sure CDM capabilities are being rolled out to keep pace with the evolving threat landscape?

The government has a checkered past when it comes to IT investments and the ability of federal agencies to provide effective cybersecurity. And while CIO's are the point of accountability on all things IT at their respective agencies, every stakeholder has to recognize their role in supporting CIOs.

But this is a hearing about finding solutions and ensuring the federal government is on the right track.

I think every agency represented today has some IT investment or application that did not produce the kinds of results the American public needs and deserves for their taxpayer dollars. And that is not to mention the profoundly damaging data breaches that have plagued federal agencies.

We have to get a handle on the cyber threat's we are facing and I believe CDM is part of the solution.

This hearing is about learning from the initial rollout and progress of CDM phase 1, plans to move through phase 2 and perhaps most importantly what is and should be the long term vision of CDM.

Obviously, part of today's hearing will involve a discussion about the resources necessary to invest in top-of-the-line security technologies.

But at its core cybersecurity is more than an issue of technology, it is an issue of governance, process, and leadership. We have to get the strategies and vision of CDM right, so that our investments don't throw good money after bad.

To that end, I intend today's hearing to include a robust conversation about the metrics necessary to measure not only the implementation of CDM but the effectiveness of the program as well.

CDM is about maintaining more secure systems and a better understanding of the risk posture of the federal enterprise. But it also represents a continuing mission and establishes the kind of structure necessary to evolve.

To that end I welcome your thoughts not only about the CDM capabilities, but also about the ultimate goal of providing network and system defenders with the data and tools necessary to do their jobs well and at the pace to combat the threats they face.

What is CDM's value add to the people on the lines of this conversation?

It is the federal agency CIO's that are ultimately accountable for bad investments or data breaches, so this is really about getting you the authorities, tools, and resources you need to get the job done.

As we continue this conversation I look forward to hearing from stakeholders as we did at last month's hearing, and what we will continue to do to make sure we are getting CDM right.

CDM is an ambitious program that I believe has the framework of providing the kind of cybersecurity the American people deserve from a government they entrust with their most valuable, personal and in some cases irreplaceable information.

I want to thank the witnesses for their time and I look forward to their testimony.

###