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

"CDM, The Future of Federal Cybersecurity?"

February 17, 2018

Remarks as Prepared

In providing effective cybersecurity, the ability of the federal enterprise to monitor and assess the vulnerabilities and threats to its networks and systems, in real time or as near real time as possible, is paramount.

This is what the Continuous Diagnostics and Mitigation – or CDM – program at DHS is all about. Understanding what and who is on federal networks so that we can achieve true visibility into the federal governments' digital ecosystem.

Phase One of CDM is to provide visibility into federal networks and information systems by working to identify what was on federal networks.

It was a simple question really: what hardware and software was on the systems an agency or department was running? This was about taking stock of those internet connected assets.

And as DHS has moved through Phase One, they found incredible amounts of devices connected to our networks that agencies were not previously aware of.

How can you protect what you can't see?

How can you modernize your technology if you don't even know what technology you have?

It is no secret that the government has trouble buying technology.

Old and outdated technology is not only a barrier to the federal government completing its mission to serve the American people in a digital world – but brings with it insecurities and raises serious cybersecurity risks for each and every agency and department.

DHS began Phase One in 2012, while I understand that setting up new government programs, buying new and advanced technologies, and deploying those technologies across a massive federal environment is not easy, the threats to federal agencies continue to grow every minute.

The maturity of the Continuing Diagnostics and Mitigation Program has to move at the pace of new technologies and innovations, not at the pace of bureaucracy.

To most effectively carryout oversight, we must educate ourselves. While DHS is working with 70 plus federal agencies and departments – from the 24 CFO Act agencies down to the dozens of smaller bureaus and offices – this Committee must work to better understand the pace at which cybersecurity technologies are advancing and how programs like CDM are working to protect .gov.

Does DHS have access to the cybersecurity platforms, technologies, and services necessary to make effective continuous monitoring a reality – in 5 years not 15 years?

We must work with the experts leading these charges in the private sector to find ways for more agile adoption of the tools and services we need to defend our networks and data.

As we have seen with both private sector and government data breaches, the identities and privacy of millions of real Americans are at risk. The federal government must work to protect the data of these citizens, including the employees that work within.

That is why we are here today. To learn what we are doing right and what we could be doing better.

And – to a certain extent – what success looks like

The rapidly evolving threat landscape of the modern information age means that government must change its processes to ensure that we aren't gathering more data than we can protect.

As we continue this conversation I look forward to hearing from stakeholders throughout the federal IT space, including technology companies, DHS and the federal agencies that they serve.

We begin with the private sector experts joining us today.

CDM is an ambitious program that I believe, if implemented well and over a reasonable timeline, provides the American people the kind of federal cybersecurity that they deserve.

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

###