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

"Assessing the State of Federal Cybersecurity Risk Determination"

July 25, 2018

Remarks as Prepared

This Subcommittee is concerned that the Federal government is not equipped to determine how threat actors seek to gain access to private information. This challenge is one of the reasons I introduced, and yesterday the Committee passed, the Advancing Cybersecurity Diagnostics and Mitigation Act. H.R. 6443 will codify and provide direction to DHS' regarding the CDM program. This was a bipartisan effort and I thank the Ranking Member, Mr. Richmond, as well as Mr. Katko, Mr. Donovan, Mr. Fitzpatrick and Mr. Langevin, for working with me on this important issue.

There is an evident lack of strategy in mitigating risk across Federal agencies. Cyber workforce gaps and legacy IT systems are vulnerabilities in the Federal government's cybersecurity posture, but the efficacy of our basic cybersecurity practices are common liabilities.

To this end, the Office of Management and Budget and Department of Homeland Security released a report earlier this year entitled "Federal Cybersecurity Risk Determination Report and Action Plan." This report spoke to many of the challenges faced in securing enterprise-wide Federal government IT systems.

Perhaps not surprisingly, OMB and DHS determined that 74 percent of government agencies have cybersecurity programs that are either at risk or high risk. The risk assessments performed by these agencies showed that a lack of threat information results in ineffective allocations of limited cyber resources. This overall situation creates enterprise-wide gaps in network visibility, IT tool and capability standardization, and common operating procedures, all of which negatively impact Federal cybersecurity.

Given the significant and ever-increasing danger of threats and the absence of good data inventory, risk management must be fully integrated into every aspect of an organization. Leaders of Federal agencies at all organizational levels must understand their responsibilities and must be accountable for protecting organizational assets and managing security and privacy risks.

The OMB and DHS Report identified four main actions that are necessary to address cybersecurity risks across the Federal enterprise. First, Federal agencies must increase their cybersecurity threat awareness. This seems like too obvious of a recommendation, but often, those charged with defending agency networks lack timely information regarding the tactics, techniques, and procedures that adversaries use to exploit government information systems.

Second, OMB urged agencies to standardize IT and cybersecurity capabilities to control costs and improve asset management. Generally speaking, agencies do not have standardized cybersecurity processes, which ultimately impacts their ability to efficiently and effectively combat threats.

The Continuous Diagnostics and Mitigation program, or CDM, will accelerate both IT management efforts and cybersecurity improvements across the Federal government. In fact, my bill, the Advancing Cybersecurity Diagnostics and Mitigation Act, will require the program to evolve to ensure agency CIO's and DHS have the visibility necessary not only to combat threats, but also to target modernization resources and efforts where they are most needed.

Third, agencies must consolidate their security operations centers to improve incident detection and response capabilities. OMB found that only 27 percent of agencies can detect and investigate attempts to access large volumes of data. This troubling statistic should cause all of us to pause. While the report identifies that Federal agencies currently lack network visibility, DHS' CDM program can assist with this issue by providing insights into what is occurring on networks. After all you can't defend what you can't see.

And finally, OMB recommended that agencies increase accountability through improved governance processes. Indeed, both the Federal Information Security Management Act and President Trump's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure already identify the agency head as the official ultimately responsible for each agency's cybersecurity. Of course, agency heads often delegate cyber risk management responsibilities to the Chief Information Officer and Chief Information Security Officer, but agency leadership should increase its oversight of, and engagement in, their agency's cybersecurity ecosystem.

Ultimately, a collaborative approach to mitigating cyber threats is meant to prioritize meeting the needs of DHS partners, and is consistent with the growing recognition among government, academic and corporate leaders that cybersecurity is increasingly interdependent across sectors and must be a core aspect of risk management strategies.

We are in an era that requires flexibility, resiliency and discipline, I look forward to a candid conversation with our witnesses about ensuring Federal networks can embody these goals. Your thoughts and opinions are important as we oversee the state of Federal government cybersecurity risks.

###