HOMELAND SECURITY
COMMITTEE

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

"The Current State of DHS' Efforts to Secure Federal Networks"
March 28, 2017

Remarks as Prepared

I see cybersecurity as one of the pre-eminent domestic and national security policy challenges of our generation, and as the Chairman of the Cybersecurity and Infrastructure Protection Subcommittee I feel especially grateful for the opportunity to work with the other Members on this panel to have a direct impact the cybersecurity posture of our country. It's a duty we do not take lightly.

Often times when the American people hear about committees performing oversight, there's a misguided perception that we're simply performing a routine check-up, taking the temperature if you will, and then moving on.

That mindset is not what compels us to meet here today.

Today's oversight is one of committed, ongoing engagement. Securing federal networks is – and rightfully should be – one of the central priorities of this Subcommittee, of this Congress, and for the American people.

While today's hearing represents a small, public facing sliver of this engagement, my commitment to all stakeholders impacted by this important issue is that our continued efforts to improve the security of federal networks will be conducted in a manner that fully recognizes the seriousness of the threats posed by our cyber adversaries. And while the stakes are indeed high, this Subcommittee is uniquely positioned to be part of the solution.

After all, the Department of Homeland Security is required, by law, to play a vital and central role in the federal government's policies, procedures, and operations for the cybersecurity of our federal agencies.

Specifically, DHS is entrusted with carrying out important legislative authorities established in the Cybersecurity Act of 2015 and Federal Information Security Modernization Act of 2014.

Ensuring the effective execution of the Department's cybersecurity initiatives has never been more important than it is today. Just last week, the Committee heard from a panel of experts about the evolving cyber threat landscape. Retired General, Keith Alexander noted, "Our increasing reliance on digital, connected devices means that while tanks, bombers, and fighter jets are certainly not obsolete, there are newer and perhaps more insidious ways of having similar effects without the need for the large investment that those assets require."

Bad actors continue to compromise the network security of both the public and private sectors at an increasingly alarming rate. From nation states like Russia, China, Iran, and North Korea and criminal organizations our systems are regularly attacked and the federal government must more effectively and efficiently anticipate these threats and do a better job protecting itself and the vast troves of sensitive information on its networks.

According to law, DHS is required to provide intrusion detection and prevention capabilities to federal agencies and work with the Office of Management and Budget to administer the implementation of agency information security policies and practices. The Department must include advanced network security tools in its efforts to continuously diagnose and mitigate cybersecurity risks. Additionally, DHS has the authority to issue Binding Operational Directives to Federal agencies in order to safeguard Federal information and information systems.

The Department's perimeter defense capabilities, known as Einstein, have progressed from monitoring, to detection, to actual prevention capabilities. A pilot is underway to examine detection technologies beyond signature-based detection, as required in the Cybersecurity Act of 2015. And, while questions about the timeline for full deployment of Continuous Diagnostics and Mitigation Program – or CDM – phases loom, breaking down the initial barriers to provide agencies with real-time situational awareness and risk-based accountable information is imperative to our Federal cybersecurity efforts.

I look forward to hearing from our witnesses today about the current status of these programs and how they will provide greater security for federal information technology systems when fully deployed.

In today's ever changing cyber threat landscape we need to ensure that these programs are agile enough to keep pace with the cybersecurity needs of federal agencies. We need to ensure DHS is properly leveraging private sector innovation and is able to quickly adopt cutting-edge technologies. We need to ensure that there is a comprehensive strategy in place, not only to engage every executive branch agency and department but also to ensure coordinated deployment.

The federal government requires the American people to submit sensitive information to its care — private financial information to the IRS, personal medical records to Medicare or the VA. We often adopt a "trust us" approach. But if we require that, then I firmly believe we must take serious steps to demonstrate our trustworthiness.

I look forward to a productive conversation with our distinguished panel of witnesses. Working together we can continue to strengthen DHS' cyber capabilities to secure Federal networks.

###