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

"Oversight of the Cybersecurity Act of 2015"
June 15, 2016

Remarks as Prepared

The Subcommittee meets today to fulfill its oversight responsibility of examining the implementation of the Cybersecurity Act of 2015 since its passage last year and to look at necessary steps going forward to strengthen our nation's cyber defenses. Congress' job doesn't end when a piece of legislation is signed into law and that is especially true when it comes to cybersecurity legislation. Continued oversight is essential to making sure the bill is implemented in a manner that actually improves our cyber defenses. If agency guidance isn't clear, if tweaks need to be made, we want to hear that feedback and address those concerns.

For that reason, we are pleased to be joined by a distinguished panel of industry experts to discuss this very important issue. Pushing the Cybersecurity Act of 2015 across the finish line last year was a significant accomplishment that was years in the making. During that time, these witnesses, and others representing critical sectors, devoted substantial energy to collaborate with policymakers on the best path forward.

Hundreds of hours of stakeholder outreach were conducted across every relevant industry group – energy, healthcare, financial services, technology, telecom, defense, retail, you name it.

In the end, the bill recognized many of the practices already deployed by these groups and codified them into law, while providing important rules of the road. My objective is to maintain that posture as we assess the implementation of the Cybersecurity Act of 2015.The bill recognized the role of DHS' National Cybersecurity & Communications Integration Center, or NCCIC, as the civilian portal for the sharing of cyber threat indicators. The key aim was to see cyber threat indicators — which contain critical information about the nature, methodology, source, and scope of cyber-attacks — shared with other parties so they can, in turn, fortify their own networks against future intrusion. In response to the devastating attack on OPM, the law also bolstered DHS' ability to deploy intrusion detection and prevention capabilities across the Federal government.

The need for a stronger cybersecurity posture is clear. Every day our country faces digital intrusions from criminals, hacktivists, terrorists, and nation-states like Russia, China and Iran. Cybersecurity is national security and the impacts of those intrusions are felt everywhere — from kitchen tables to American businesses. We cannot tolerate acts of cyber theft and cyber warfare, especially when they result in the theft of intellectual property and innovation, and put our nation's critical infrastructure at risk.

We cannot sit idly by while escalating ransomware attacks on hospitals and healthcare providers threaten our citizens by locking out access to medical records. Cybersecurity breaches and data manipulation can undermine consumer confidence and damage a company's hard earned reputation in a matter of seconds. And while we have yet to see a major corporation completely collapse due to a cyber-attack, the possibility is no longer science fiction. One can only imagine the turmoil that would be caused should Americans' checking accounts suddenly be drained. Loss of trust in our financial system would cause an economic meltdown. Nearly a third of CEOs surveyed identify cybersecurity as the largest issue impacting their companies today and only half say they are fully prepared for a cyber event. There are two types of companies: those who have been hacked and those who don't know they have been hacked. This is why Congress passed the Cybersecurity Act last year. Information sharing between companies, the government, and critical sectors improves our ability to defend against these attacks.

Beyond the impact on the private sector, safeguarding cyberspace is also one of the great national security challenges of our time – and the American people recognize this. In fact, in a recent Pew Research Poll, Americans named cybersecurity as their second biggest perceived threat only to ISIS. Imagine a catastrophic cyber attack on our gas pipelines or the power grid. Such assaults on our critical infrastructure could cripple our economy and weaken our ability to defend the United States. Our adversaries are hard at work developing and refining cyber attack capabilities and they are using them to intimidate our government and threaten our people.

But the threat extends beyond the industrial engines that drive our economy, to the homes of Americans themselves. Criminals and countries alike can use cyber attacks to raid Americans' savings accounts or steal their personal health records. The recent breach of Anthem demonstrated the very real capability and intent of bad actors to prey upon Americans' most sensitive information. We cannot leave the American people, the American economy, and our critical infrastructure to fend for itself.

That's why Congress passed the Cybersecurity Act of 2015. This new law strengthens DHS's ability to more effectively secure government networks and incentivizes the sharing of cyber threat indicators among critical sectors and with the government to bolster protections from future attacks. Information is the currency of today's age, and we must constantly work together across all sectors if we expect to stay one step ahead of the adversaries on this new battlefield.

Congress must utilize rigorous oversight to ensure that DHS is fulfilling its mission to better protect our networks, and that's why we're here today. I want to thank the witnesses for testifying before this subcommittee and I look forward to your testimony.

###