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

Emerging Cyber Threats to the United States
February 25, 2016

Remarks as Prepared

The Subcommittee is meeting today to examine the evolving cybersecurity threats from nation-states such as China, Russia, North Korea and Iran, as well as cyber threats from criminal organizations and terrorist groups such as ISIS. Over the last several years we have seen these actors continue to develop and build even more sophisticated cyber capabilities. In 2016, these hackers pose an even greater threat to the U.S. homeland and our critical infrastructure. To put it simply, cybersecurity is national security.

In 2015, the nation was victim to one of the most significant cyber attacks in history. The breach at the Office of Personnel Management exposed the personal and extremely sensitive security clearance information of 21.5 million current and former government employees. In 2014, we saw North Korea conduct a cyber attack on Sony Pictures that not only destroyed computers, but also sought to muzzle free speech and threaten American ideals.

Unfortunately, the Administration's lack of proportional responses to these cyber attacks has demonstrated to the world that there are no real consequences for such actions. Without a comprehensive national cybersecurity strategy that addresses deterrence effectively, I worry that 20l6 could bring an increasing number of those willing to push the boundaries.

In recent news, a lot of attention was directed at the Hollywood Presbyterian Medical Center in Los Angeles that was a victim of a ransomware attack. This type of malware infects victims' computers and locks them until a payment, or a "ransom," is made. The medical center was forced to pay $17,000 to restore its systems. But this isn't unique to Hollywood. In my own district in Northeast Texas, the Titus Regional Medical Center suffered a similar attack. Their electronic health record system was locked and they weren't able to access patient information.

Of the nation-state threats, Russia continues rank near the top in terms of capabilities, with increasing aggression across the globe that may continue to manifest itself in cyberspace. The Director of National Intelligence, James Clapper, told the Senate Armed Services Committee in September that the Russian government is establishing its own central cyber command that will be responsible for carrying out offensive cyber operations.

China also ranks high in terms of capability and continues to pose a significant threat to the U.S. in terms of cyber espionage and theft of intellectual property. In September, the Administration

announced an agreement with the Chinese government to refrain from engaging in hacking of intellectual property. I look forward to hearing today from our industry witnesses today on their thoughts about the success of this agreement.

Iran continues to emerge as a top cybersecurity threat. While many would argue that its intent to carry out attacks is strong, it still lags behind other nation-states in capabilities. However, the Administration's recent nuclear agreement with Iran could have unintended consequences in cyberspace, as the lifting of economic sanctions could provide influx of cash to fuel the development of cybersecurity capabilities.

Criminal organizations continue to pose a great risk to the American people, as we have seen with the breaches of Target and Home Depot, which exposed the credit card information of millions of people. While the intent of criminal groups may be different from nation-states, the impact on everyday Americans is felt very directly.

Lastly, terrorist groups such as ISIS may currently lack the capability to pose a major cybersecurity threat to U.S. But given the vast resources the group has amassed, developing or purchasing sophisticated cyber tools is not far out of reach. ISIS followers and the so-called Cyber Caliphate have had success in hacking social media accounts of military personnel and posting home addresses and other personal information online asking followers to carry out attacks.

In late 2015, Congress—recognizing these threats—enacted the Cybersecurity Act of 2015. The Act establishes the Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) as the sole civilian interface for sharing of cyber threat information with the Federal government. The Act establishes liability protections for companies to share information with DHS, and among themselves. In light of this legislation, we hope the private sector will share more with each other and the government, and we look forward to hearing from our witnesses on what they are doing to increase information sharing.

In response to the devastating attack on OPM, the Act bolsters DHS' ability to deploy intrusion detection and prevention capabilities across the Federal government. These capabilities will ensure the proper capabilities to defend government networks from these nation-state attacks.

Unfortunately, cyber threat actors—be they nation states, criminal groups, or terrorist organizations—remain undeterred, continuing to conduct cyber attacks. This problem is compounded by the lack of acceptable norms in cyberspace and I have questions on whether or not the Administration's lack of response to these attacks has deterred or emboldened our adversaries. The President recently announced a Cybersecurity National Action Plan. Whether this is too little too late, and the clarity of the overall guidance behind the plan, remains to be seen as we watch the most meaningful part of any grand plan: the execution. In this day in age, there is agreement that the battle for the security of our information systems is continually escalating. The testimony today will help inform what actions Congress can take to further the interests of our national security.

###