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

"Examining DHS's Cybersecurity Mission"

October 3, 2017

Remarks as Prepared

We are here to today, at the start of National Cybersecurity Awareness Month, to discuss what I believe is one of the defining public policy challenges of our generation – the cybersecurity posture of the United States. We have seen cyberattacks hit practically every sector of our economy with devastating impacts to both government agencies and the private sector alike – and it's our shared duty to ensure we're doing our best to defend against the very real threat our cyber adversaries pose.

But make no mistake – the cybersecurity challenges we face are about much, much more than simply protecting bottom lines, or intellectual property, or even our nation's most classified information. They also impact the personal, often irreplaceable information, of every American.

This year, we've seen – on a grand scale – just how much damage can be done by a single individual or entity looking to conduct a cyber attack. It may take only one bad actor and only one exploitable vulnerability to do something such as compromise the information of 143 million Americans.

This is not the first cyber attack that's garnered national headlines, and unfortunately – it almost assuredly will not be the last.

As the members of this panel and as our witnesses here today know well, there is no silver bullet or guaranteed technology to "fix" the cybersecurity problem. Rather, this is part of an ongoing, sustained, and comprehensive campaign to ensure the United States remains the world's cybersecurity superpower.

We will continue to need a sharp workforce, the collective efforts in public-private partnerships, and the leadership of our government agencies to leverage our resources and counter our highly sophisticated cyber adversaries.

Today, this Subcommittee meets to hear from the government officials charged with meeting these cyber threats. These are the folks on the front lines day in and day out.

DHS is the federal government's lead civilian agency for cybersecurity, and within it, the National Protection and Programs Directorate, or NPPD, leads our national effort to safeguard and enhance

the resilience of the nation's physical and cyber infrastructure, helping federal agencies and, when requested, the private sector harden their networks and respond to cybersecurity incidents.

NPPD partners with critical infrastructure owners and operators and other homeland security enterprise stakeholders to offer a wide variety of cybersecurity capabilities, such as system assessments, incident response and mitigation support, and the ability to hunt for malicious cyber activity.

This collaborative approach to mitigating cyber incidents 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.

This Committee has been working hard to ensure that NPPD – and DHS in its entirety – has the necessary authorizations and organization it needs to combat growing cyber threats.

DHS needs a robust workforce and an efficient organizational structure to support both its cybersecurity and infrastructure protection missions.

Earlier this year, this Committee marked up and passed H.R. 3359 – the Cybersecurity and Infrastructure Security Agency Act of 2017 to reorganize and strengthen NPPD.

As the cyber threat landscape continues to evolve, so should DHS, and in doing that, H.R. 3359 is the tool we'll use to bring "NPPD" to a more visible role in the cybersecurity of this nation.

As a committee, and as a Congress, we have taken important steps in the right direction with legislation on information sharing, modernizing the federal government's information technology, and in getting our state and local officials the cybersecurity support they need.

Some of these programs have been years in the making.

Real-time collaboration between the government and the private sector is a lofty and worthwhile goal. Through the Automated Indicator Sharing program, or AIS, DHS has been partnering with industry to create and enhance that broader information-sharing environment – and we've made progress in the right direction.

While we know that proactive information sharing is only as good as the information being provided, that type of relationship can only be made possible with a strong foundation of trust.

I'm looking forward to a robust discussion today, not only about how the Department can be best organized and equipped to ensure that we are leveraging the resources of the federal government towards this immense challenge, but also how the government can forge and grow the necessary partnerships to achieve greater cybersecurity for our nation.

We have to get this right because new technologies – the internet of things, driverless cars, artificial intelligence, and quantum computing – are rapidly evolving.

We need to be securing at the speed of innovation – not of bureaucracy.

Because we are in an era that requires flexibility, resiliency and discipline and I hope I will hear those values operationalized in the forthcoming testimony.

Cyberspace plays an increasingly dominant role in the fabric of our society, and it will take continual collaboration across the public, private, international and domestic spaces to keep making the advancements needed to prioritize cybersecurity for our country.

I know this is a responsibility that everyone on this subcommittee takes extraordinarily seriously, and I look forward to the discussion today with our witnesses.

###