



Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

March 4, 2015

Media Contact: April Ward
(202) 226-8477

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

“Industry Perspectives on the President’s Cybersecurity Information Sharing Proposal”

Remarks as Prepared

The subcommittee meets today to hear from key stakeholders including industry, privacy advocates, and academia on the president’s cybersecurity information sharing proposal and recent cyber initiatives. Last week, the full committee heard testimony from the Department of Homeland Security’s top cyber officials on the growing cybersecurity threat and how this legislative proposal could enhance protection of our digital networks and Americans’ most personal information. Today, we turn to the private sector and look forward to hearing from our witnesses on what they think cyber threat sharing legislation should look like.

For years, the private sector has been on the front lines battling devastating cyber attacks from criminals, hackers, and nation-states such as Iran, China, Russia, and North Korea. Any cyber threat sharing legislation produced by Congress should enhance existing capabilities and relationships while establishing procedures to safeguard personal privacy.

Protecting privacy and the integrity of information is what compels us to act. The recent cyber breach of health insurance giant Anthem exposed the personal information of up to eighty million individuals—approximately one in four Americans—demonstrating that the quantity and sophistication of these attacks are only increasing. Just last week, Director of National Intelligence, James Clapper underscored this fact, stating that “[cyber] attacks against us are increasing in frequency, scale, sophistication and severity of impact” and “the methods of attack, the systems targeted, and the victims are also expanding in diversity and intensity on a daily basis.” He emphasized that privacy and the integrity of information are indeed at risk, stating, “in the future, we’ll probably see cyber operations that change or manipulate electronic information to compromise its integrity instead of simply deleting or disrupting access to it.”

Director Clapper also revealed that in 2014, America “saw, for the first time, destructive cyber attacks carried out on U.S. soil by nation-state entities,” confirming that Iran was behind a cyber attack against the Las Vegas Sands Corp., which is owned by a vocal supporter of Israel.

These breaches are becoming the norm, with attacks on Sony Pictures, Target, Home Depot, JP Morgan, and many others. FBI Director James Comey stated, “There are two kinds of big companies in the United States. There are those who’ve been hacked by the Chinese and those who don’t know they’ve been hacked by the Chinese.” Further, these attacks are not just affecting the largest businesses and financial institutions, but small and medium ones as well. As such, we need to pass legislation that facilitates the sharing of cyber threat indicators and contains robust privacy protections to improve collaboration between federal civilian agencies like DHS and the private sector.

The Department of Homeland Security’s National Cybersecurity and Communications Integration Center, or NCCIC, has been at the forefront working with the private sector to facilitate cyber threat sharing between the government and the private sector. NCCIC is a civilian cyber operations center with an embedded statutorily-required privacy office. In fact, both industry and privacy advocates support NCCIC, which was codified into law last year in bipartisan legislation produced by this committee.

NCCIC has been the lead civilian portal for cyber threat sharing between the private sector and the government and it is important that NCCIC and other civilian portals be the focus of any cyber threat sharing legislation.

Today, many companies still choose not to share cyber threat indicators with one another or NCCIC because they fear legal liability. Information about an attack experienced by one can enable another to fortify its defenses. Yet when this sharing does not occur, it leaves all of us more vulnerable because the same criminals can use the same tactics to target other companies, exposing even more Americans to having their private information compromised.

Past legislative attempts to improve cyber threat sharing between the private sector and government, and private sector-to-private sector, have failed in large part because they could not balance privacy protections with the need for industry to share cyber threat indicators. This Congress, I look forward to working with Chairman McCaul, Ranking Member Thompson, and Ranking Member Richmond to craft thoughtful cybersecurity legislation that achieves this balance.

I look forward to hearing from each of the witnesses in their respective fields about their opinions on how best this committee should move forward on drafting legislation to address these issues and what perspectives each of you have on the president’s recent legislative proposal and cyber initiatives.

Every generation faces monumental moments where their tenacity to overcome the challenges of the time are tested. Now is our time, as we move deeper into the digital age, to ensure that the cybersecurity challenges we face today are met with the same resolve shown by previous generations of Americans.

I want to thank the witnesses for testifying before this committee and I look forward to your testimony.

###