



Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

July 28, 2015

Media Contact: Susan Phalen
(202) 226-8477

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

“Promoting and Incentivizing Cybersecurity Best Practices”

Remarks as Prepared

The Subcommittee is meeting today to examine the potential benefits of expanding the Support Anti-Terrorism by Fostering Effective Technologies Act, referred to as the SAFETY Act, to clarify that, on a voluntary basis, cybersecurity products and services can be reviewed and certified to receive enhanced liability protections for large-scale cyber incidents.

Right now, our cyber defenses are weak and because addressing cybersecurity vulnerabilities is costly, we need to find ways to promote and incentivize investment in cybersecurity. We need to incentivize companies to have a robust cyber risk management plan in place.

Through this hearing, we want to hear from our expert witnesses if the SAFETY Act Office at DHS could be leveraged to promote and incentivize cybersecurity best practices within its existing framework. By way of history, the SAFETY Act was part of the Homeland Security Act of 2002, and is a voluntary program that currently provides incentives for the development and deployment of anti-terrorism technologies.

The SAFETY Act ensures that the threat of costly litigation does not deter potential manufacturers or sellers of anti-terrorism technologies, at both small and large companies, from developing and putting into the marketplace products and services that could reduce the risk or mitigate the consequences of a large-scale terrorist event. Companies qualify for the protections afforded by the SAFETY Act by demonstrating, through an ongoing basis, that they have a comprehensive and agile risk management plan. Applicants to this voluntary program must submit to a rigorous and thorough vetting process by DHS’ SAFETY Act Office in order to receive liability protections in the event of an act of terrorism.

Homeland security and national security challenges are constantly evolving and the cybersecurity threat is rapidly growing. It is in that capacity that earlier this year we passed HR 1731, the National

Cybersecurity Protection Advancement Act. The goal of that legislation, which passed the House with a bipartisan vote of 355-63 and is now awaiting Senate action, is to strengthen the sharing of cyber threat indicators to guard against criminal groups, hacktivists, or Nation- State actors.

Separately, we have been meeting with stakeholders to find other ways to strengthen cybersecurity, including expanding the SAFETY Act for cyber purposes. Right now the SAFETY Act can only be triggered by an act of terrorism. However, for cyber attacks attribution is extremely difficult to determine. Regardless of whether the hacker was a terrorist, nation state, cyber criminal, or hacktivist, the impact of a devastating cyber attack would be the same. If there is something more that can be done to increase cybersecurity best practices overall, and potentially reduce the likelihood of large-scale cyber attack, this Subcommittee is going to examine it. SAFETY Act coverage for cybersecurity will not solve all our cybersecurity challenges but it has the potential to make a significant improvement in our Nation's cyber defenses.

In the coming weeks, the Committee on Homeland Security will consider House-passed legislation from the 113th Congress that would amend the SAFETY Act to establish a "qualifying cyber incident" threshold to trigger SAFETY Act liability protections for vetted cybersecurity technologies.

The very creation of the Department of Homeland Security stemmed from the attacks on September 11, 2001. While we must and will remain vigilant and do everything we can to prevent another, devastating attack on Americans, we must also recognize that the threat landscape is changing. Cyberspace is in many ways the new frontier, and a "cyber 9/11" is only a matter of time if we fail to strengthen our cyber defenses. So we need to ensure that we are doing everything possible to harden our defenses "left of boom", as they say in military parlance.

This potential legislation has the potential to increase investments in the security and resilience of our Nation's critical infrastructure, including the power grids, air traffic control, and banking systems. Much of our Nation's critical infrastructure is privately owned, and in the 21st century there now exists an interconnectedness of physical security and cybersecurity. This means that someone sitting at a keyboard can now initiate a physical injury by issuing commands to an office building, air traffic control system, or someone's automobile, resulting in loss of life- not just the theft of personal information from a database.

Many products and services weren't built with cybersecurity in mind. This is why we need to incentivize market-driven solutions to raise the bar on how we manage our cybersecurity risks. Fortunately, the United States is home to an ingenious entrepreneurial culture and the best high tech companies in the world who have developed products and services that can help improve the information security resilience of our critical infrastructure and for companies that improve our quality of life.

If amending the SAFETY Act to include "qualifying cyber incidents" would better safeguard our Nation, and potentially prevent a cyber attack that could shut things down and bring commerce to a screeching halt, then we owe it to our constituents to examine the potential benefits it could provide. This is especially true given the increasing importance of cybersecurity in the lives of every American.

###