Rep. Will Hurd Opening Statement
Subcommittee on Information Technology
Federal Cybersecurity Detection, Response, & Mitigation
April 20, 2016

Good morning, everyone.

Every day, federal agencies face a barrage of attacks on their information systems from a number of different actors. Attacks on both the public and private sectors consistently reveal one common truth – no one is immune.

In December of last year, Juniper Networks announced that malicious code had been placed in its ScreenOS software, leaving a gaping vulnerability in one of its legacy products.

This particular vulnerability may have allowed outside actors to monitor network traffic, potentially decrypt information, and even take control of firewalls. Within a matter of days, the company provided its clients—which include various U.S. intelligence entities and at least twelve federal agencies—with an "emergency security patch."

DHS and other law enforcement agencies acted swiftly to notify federal agencies of the breach and Juniper's security advisory. Both of their actions may have averted a potentially devastating breach of sensitive data. This is just one sophisticated example of the attacks that U.S. companies and their federal clients face on a daily basis.

In January of this year, the Committee sent letters to the heads of 24 federal agencies requesting an inventory of systems running the aforementioned software. Additionally, the Committee asked for an update on their progress in installing the corresponding security

patch.

Of the twelve agencies affected, three, including the Department of Treasury, took longer than fifty days to fully install patches and mitigate the threat posed by this vulnerability.

This is absolutely unacceptable.

The inability of federal agencies to maintain a comprehensive view and inventory of their information systems and respond to Congress in a timely manner cannot be the status quo.

Last December, Congress passed landmark information sharing legislation, the Cybersecurity Act of 2015, which creates a voluntary cybersecurity information sharing process to encourage public and private sector entities to collaborate and share information. Moreover, the bill established the Department of Homeland Security as the sole portal for companies to share information with the federal government.

With their newly codified role, I look forward to working with Dr. Ozment and DHS on how to strengthen their own posture and ensure that they possess the necessary technical tools to detect and mitigate threats and disseminate threat information within the federal government.

Only by fostering this framework where government and private entities are able to freely share knowledge of security vulnerabilities, threat indicators, and signatures can we be sure that our network defenses are getting the best intelligence available.

In addition, we must continue to learn from the private sector. Industry leaders like ThreatConnect and FireEye are constantly pushing the envelope in what is possible in cybersecurity. The

government should not seek to compete with them, but rather should harness these engines of innovation, learn from them, and safely cooperate with them under the guidance of good sense and personal liberty.

I hope that this hearing will serve as the starting line for a larger conversation on attribution. Various international groups and state-sponsored actors are constantly attempting to steal military secrets and expose the personally identifiable information of American citizens, and we cannot stand idly by while this happens. I believe that attribution is a form of deterrence.

This hearing presents an opportunity to learn how federal agencies can improve their overall cybersecurity postures, share more timely and relevant information, and work with the private sector in a way that benefits all involved, while respecting the institutions of commerce and privacy.

I welcome our witnesses and look forward to hearing your testimony today.