Chairman Johnson's Opening Statement
"Cybersecurity Regulation Harmonization"
Wednesday, June 21, 2017

As submitted for the record:

Cybersecurity is one of this Committee's top priorities. Today's hearing is our fifth hearing examining this threat. In other hearings on this topic we explored the importance of information sharing and the need for liability protections; the OPM and IRS data breaches; and the broad cybersecurity threat landscape—criminal attacks, malicious attacks, industrial espionage, and cyber warfare.

The Committee has also highlighted one of the greatest impediments to the U.S. economy realizing its full potential: our regulatory burden. According to the Competitive Enterprise Institute, the total annual federal regulatory cost amounts to $2 trillion. To put this in perspective, this burden amounts to approximately $15,000, per year, per household. There are only seven economies in the world that are larger than the regulatory burden we impose on our economy and American families.

Today's hearing considers both of these problems. Cyber threats are real and growing. As they have evolved, so has the response from government regulatory bodies. Though these efforts are well intended, the result has been a myriad of duplicative, sometimes conflicting, rules imposed on industries throughout the economy. Not only do these rules impose regulatory costs, but they can also lessen security, as companies spend limited time and resources concentrating on regulatory compliance at the expense of security. As an example, one financial services firm reports that 40 percent of its time is spent on regulations and reporting requirements, time better spent enhancing the security of its networks.

In December, I had the opportunity to meet with Dr. Eviatar Matania, the Director General of Israel's National Cyber Directorate. Dr. Matania established a comprehensive cyber strategy for Israel with a direct reporting line to the Prime Minister. The United States would be well served by evaluating Israel's approach and look for opportunities to harmonize the federal government's approach to cybersecurity to ensure consistent, effective, and non-duplicative rules of the road.

We also should re-prioritize our efforts. At our last cybersecurity hearing, former Assistant Director of the FBI Cyber Division Steven Chabinsky testified that:

> We should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response—that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail. For this to occur, we will need to reconsider how we fund cybersecurity efforts. . . . Our underfunding threat deterrence also hurts the private sector, which largely has been left to fend for itself. One financial institution disclosed that it planned to spend $600 million and dedicate 2,000 employees to cybersecurity last year.

Today, witnesses from financial services, the tech sector, healthcare, and state government will explain exactly how they are fending for themselves—both in securing their networks and in responding to the current diffuse regulatory landscape. I want to thank all of these witnesses for being here today, and I look forward to your testimony.