**U.S. Senate Homeland Security and Governmental Affairs Committee**

**"Cybersecurity Regulation Harmonization"**

**June 21, 2017**

**Ranking Member Claire McCaskill**

**Opening Statement**

Thank you, Chairman Johnson. One of my top priorities as a senator is focusing on how we can make government work better and more efficiently. I have spent my career concentrating on eliminating waste, fraud and abuse in an effort to save taxpayer dollars and improve government services.

Today's hearing allows us to hear from representatives from the private sector and the states about how they manage compliance with the variety of regulations they face related to data and cybersecurity. There is currently no clearinghouse for mitigating conflicts between regulators, and as a result, states and industry bear the burden for ensuring compliance between sometimes redundant and conflicting regulations.

Regulators play an essential role in mandating security measures, like notifications after a data breach and requiring a minimum level of security to protect personally identifiable information. However, as these witnesses

will attest, while the goal of the regulations is improved security, due to a lack of harmonization between regulations, industry spends valuable time sorting through compliance when it could be investing those hours and resources into improving their systems and services.

We'll hear today how centralization of IT systems can play a key role in improving efficiency and security. The same can be said about centralizing cyber policy across the federal government. We have made significant strides in recent years to authorize and operationalize the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). President Obama also mandated the creation of the NIST Cybersecurity Framework, which creates a common language for government and industry.

We have spent years working to make DHS the central cybersecurity information sharing entity in the federal government. We finally passed the Cybersecurity Information Sharing Act (CISA) in 2015, providing liability protection to encourage industry to share threat information with DHS. But now, the Department of Health and Human Services (HHS) has decided that the NCCIC and the existing information sharing structure have limitations. Rather than examining what the private sector was doing to address potential

gaps, HHS went ahead and built a health-specific version called the Health Cybersecurity and Communications Integration Center, referred to as the HCCIC. Talk about duplicative.

I have questions about the utility of this new entity. It also is not clear to me that this new HHS cyber center is necessary or that it adds value. We should be looking to enhance information sharing participation and the NCCIC's capabilities, not sprouting a "kick" for each industry or critical infrastructure sector.

I'm glad Chairman Johnson is joining me in sending a letter to HHS asking questions about the genesis of the HCCIC, how it has been and will coordinate with DHS, information on the liability protections offered to those that share information with the HCCIC, and why this new entity is necessary.

I look forward to hearing from the witnesses today about other ways we can work to simplify and harmonize their regulatory burden. Thank you.