"What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity"
Opening Statement of Chairman Ron Johnson
February 11, 2020

As prepared for delivery:

The purpose of today's hearing is to examine how state and local governments and critical infrastructure owners/operators and other businesses can mitigate, and protect against, persistent cyber threats.

The protection of mission-critical systems for state, local, tribal, and territorial (SLTT) governments is an essential component of our nation's cybersecurity. Last year alone, cybercriminals used ransomware attacks to cripple municipal entities with near impunity. An estimated 966 government, education, and healthcare entities were victims of ransomware attacks in 2019 that cost an estimated $7.5 billion in operational and financial damages.

In addition to the increased frequency of ransomware attacks, heightened tensions between the U.S. and Iran have raised concerns about the extent to which state and local governments, and critical infrastructure owners and operators, are prepared to respond to cyberattacks by state or state-sponsored actors. Earlier this year, DHS issued multiple alert bulletins referencing potential Iranian cyberattacks against our critical infrastructure in retaliation for the U.S.'s lethal strike against Qassem Soleimani, then head of Iran's Islamic Revolutionary Guard Corps, a designated Foreign Terrorist Organization. One bulletin referenced Iran's "willingness to push the boundaries of their activities, which include destructive wiper malware and, potentially, cyber-enabled kinetic attacks."

Fortunately, according to Leidos, a defense, science, and information technology research company, "[a] handful of hygiene measures can stop up to 95 percent of targeted cyber intrusions." In other words, simple, cost-effective actions can make a tremendous difference. In addition to practicing good cyber hygiene, SLTT governments, and critical infrastructure owners and operators can also leverage Department of Homeland Security resources to help further protect their cybersecurity systems and assets. DHS, specifically the Cybersecurity and Critical Infrastructure Security Agency, plays a key role in sharing cyber threat information and cyber hygiene practices. The Department also offers assistance to help these entities better protect their mission-critical systems, such as penetration testing, and it also offers recovery assistance if an incident does occur.

State and local governments and the private sector are on the front lines and grappling with these cyber threats every day. For example, this past August, Texas was hit by a coordinated ransomware attack. The ransom was not paid, but the response effort still cost the state hundreds of thousands of dollars. DHS assisted in the response through reverse engineering the malware, but according to state officials, additional improvements are needed. We can learn a great deal from the experiences of individual states and businesses, and identify areas for improvement.

I want to thank all of the witnesses for being here today, and I look forward to your testimony.