Opening Statement of Chairman Ron Johnson

"Under Attack: Cybersecurity and the OPM Data Breach"

June 25, 2015

As prepared for delivery:

Good morning, and welcome.

Earlier this month, the Office of Personnel Management (OPM) announced that over the past year hackers stole 4.1 million federal employees' personnel records. Then, just days later, we learned the attack was actually far broader, involving some of the most sensitive data the federal government holds on its employees, and likely, many more records. It is hard to overstate the seriousness of this breach. It has put people's lives and our nation at risk.

This massive theft of data may be the largest breach the federal government has seen to date. But it's not the first data breach affecting federal agencies, or even the OPM. Unfortunately, I doubt it will be the last. Our nation is dependent on cyber infrastructure and that makes our future vulnerable. The cyber threats against us are going to continue to grow—in size and sophistication.

The purpose of this hearing is to lay out the reality of that cyber threat and vulnerability. The first step in solving any problem is recognizing and admitting you have one. We must acknowledge we have a significant cybersecurity problem in the federal government, especially at the OPM. This intrusion on the OPM's networks is only the latest of many against the agency, and the OPM has become a case study in the consequences of inadequate action and neglect.

Cybersecurity on federal agency networks has proved to be grossly inadequate. Foreign actors, cyber criminals and hacktivists are accessing our networks with ease and impunity. While our defenses are antiquated, our adversaries are by comparison proving to be highly sophisticated. Meanwhile, agencies are concentrating their resources trying to dictate cybersecurity requirements for private companies, which in many cases are implementing cybersecurity better and more cheaply.

The OPM has been hacked five times in the past three years, and it still has not responded to effectively secure its network. Today's hearing will focus on the two most recent breaches.

We will hear from the OPM Inspector General, Mr. Patrick McFarland, that the OPM has continued to neglect information security, which may have contributed to these breaches. We will hear from Dr. Andy Ozment about the specifics of this attack, as well as the Department of Homeland Security's role in federal cybersecurity. Mr. Tony Scott will testify about efforts on cybersecurity across the government and about the information security requirements of federal agencies. Finally, we will give OPM Director Katherine Archuleta an opportunity to explain how this happened on her watch, to let us know who she believes is responsible, and to clarify what we can expect from the OPM going forward.

There’s a bullseye on the back of USA.gov, and it does not appear this administration is devoting enough attention to this reality. We need leadership to develop and implement an effective plan to stop future cyberattacks. Without effective cybersecurity, our nation will not be safe and secure. Cybersecurity must be a top priority.

Thank you. I look forward to your testimony.

###