Opening Statement of Chairman Greg Walden
Subcommittee on Energy
Hearing on "The Electricity Sector's Efforts to Respond to Cybersecurity Threats."
February 1, 2017

(As prepared for delivery)

One of the humbling responsibilities for members of the Energy and Commerce Committee is to fully appreciate the power we have to make policy changes that can have enormous and positive impacts on American consumers for decades to come. From health care, to manufacturing and trade, to telecommunications, transportation, and the delivery of energy, our goal is to identify how to position the United States to harness the tremendous potential of digital communications for all sectors of the economy, while minimizing unintended side effects.

We are witnessing the transformation of American commerce as advances in digital and information technology affect almost everything that we do in our daily lives. And we see how layering new digital ways of doing things onto existing practices and infrastructures creates new risks and potential harm. Who among us is not frequently seeking out a plug in so that we can keep our various electronic devices charged? Never has the reliability of the electric grid been more important to everything in our lives. That also means never has the electric grid been more of a potential target for disruption by nefarious actors. The hearing today concerns what is being done to address and respond to the cybersecurity threats to our nation's electricity system.

By any measure, the reliable supply of electricity is an essential part of almost everything we do, and its loss—even for short periods—can have expensive and

life threatening consequences. Unfortunately, cyber threats in this sector are unavoidable and growing.

This is due to the dynamic nature of the information flows in the modern world as well as the increasing sophistication of hackers and adversaries. Threats in these flows will only grow as the instant information and communications enabled by digital technology become more essential for our electricity system to operate at increased levels of reliability.

Looking forward, it is clear the growth of digital technology will constantly introduce new avenues for cybersecurity threats that must be managed effectively. Responsibility for addressing these threats, while harnessing the promise of digital technology, rests largely on the thousands of people involved in planning and operating our nation's complex electricity transmission systems, as well as the organizations charged with ensuring reliability.

This morning we will hear from industry and cybersecurity experts who can provide us a report on the state of cybersecurity planning and practices. Our witnesses will help us understand just what is being done to address cybersecurity threats, and how the industry plans to confront new threats as they emerge.

The hearing will help us begin to understand more fully where the electricity sector is and where it should be in terms of cybersecurity and related risks to electric reliability. This will lay the groundwork for closer scrutiny of the relevant policies necessary to ensure future reliability in an evolving electricity sector.

There are many questions to pursue: How is cybersecurity planning being embedded in procurement and other systems planning by the industry? What

measures are being implemented to prepare for successful attacks, so that—just as with nature's constant threats—if the lights do go out, can we get them on quickly? What is being developed to address the truly high consequence but low probability events that can have the most devastating impacts? And what more can be done?

As the committee implements its own energy policy agenda, the testimony we take will inform how we approach the future and how we best use innovation and technology to protect American consumers.

###