Opening Statement of the Honorable Fred Upton
Subcommittee on Energy
Hearing on "The Electricity Sector's Efforts to Respond to Cybersecurity Threats"
February 1, 2017

(As prepared for delivery)

Today's hearing will examine what the electricity sector is currently doing to prepare for and respond to cybersecurity threats to the nation's electricity transmission systems.

News reports bombard us almost daily about malware infections and portrayals of the harm from cyber attacks. We've read alarming descriptions of what might happen if there is successful, widespread attack on the critical infrastructure of the electricity system—and the potential challenges to recovering from such an attack.

It is unquestionable that ensuring the reliable supply of electricity is absolutely vital to our nation's security, economy, our health and welfare.

In my home state of Michigan and across the country, electricity enables telecommunications, financial transactions, the transport and delivery of energy, food. It powers the infrastructure that delivers our drinking water. It enables business and industry to make and provide the goods and services of our modern society. It powers our hospitals, our households.

So cyber threats to reliability deserve our constant examination. But as we do so, we should also recognize that ensuring reliability *is* the central function of electricity grid operations—and a tremendously complex system has developed over time to ensure our lights stay on. Given the unique nature of electricity, the system operates to address the occasional loss of transmission components and to avoid cascading failures; it doesn't always succeed, but large scale blackouts have been rare for a reason.

Nevertheless, new risks are emerging rapidly. The integration into the system of new technologies—especially digital technologies—that are essential for keeping up with our nation's energy needs constantly add new vulnerabilities. Combine this with the rapid development of cyber threats and safeguarding transmission infrastructure becomes particularly challenging.

In recent years, Congress has enhanced the ability of the electricity sector to address emerging cyber and physical threats. In the last Congress, this Committee wrote provisions included in the FAST Act that sought to facilitate sharing of threat information between private sector asset owners and the federal government. Other measures enhanced authorities for taking emergency action against cyber and physical attacks.

At the same time, the North American Electric Reliability Corporation (NERC)—operating through authorities authored by this Committee—has been establishing and enforcing critical infrastructure protection standards and coordinating a number of other activities to confront these threats. Industry and federal authorities have also been working to address risks.

We've taken testimony that outlines these activities in recent years. And I think the evidence shows that utilities and transmission operators are not sitting still.

But I don't believe anybody will dispute that improvements in operational practices, information sharing, defensive planning, supply chain controls, hardening of infrastructure remain necessary. And nobody will dispute that someday, an attack may succeed in taking down critical components; how does the industry plan to respond to that?

Today's hearing will update the subcommittee on the state of the various NERC and industry activities to mitigate risks and respond to cyber attacks. This will inform two objectives:

First, the energy subcommittee's agenda for this Congress will include a close focus on the various structural, economic, and technological factors that are affecting development of the nation's electricity system.

We'll be examining policies that may need to be reformed to ensure this system adequately meets the demands of consumers in coming decades. And a key aspect of any of this work will involve enhancing reliability in the evolving electricity system to meet the demands of the digital age.

And second: we must continue to build a record about electric sector efforts to address cyber security threats. This will help the subcommittee identify whether additional measures, are necessary. In time, we will hear from DOE, FERC and

other agencies, but developing a clear picture today about what the industry actually is doing will be critical to this ongoing effort.

With that as a backdrop, let me welcome our witnesses. Our panel today provides a number of important perspectives: We'll hear from NERC, the industry's reliability organization responsible for setting and enforcing standards; we'll hear how the industry coordinates cybersecurity planning and response; we'll hear perspective from a critical infrastructure expert; and we'll hear from somebody responsible for cybersecurity in the actual operations of transmission systems.

The panel this morning should help cover a range of topics—from security standards to information sharing and recovery planning. It should help us discuss the various levels of cyber and related physical risks to electricity infrastructure and how they are addressed. And it should help us understand where gaps may be going forward.

###