Opening Statement of Republican Leader Greg Walden
Subcommittee on Energy
"Keeping The Lights On: Addressing Cyber Threats to the Grid"
July 12, 2019

As Prepared for Delivery

Thank you, Mr. Chairman.

By any measure, the reliable supply of electricity is an essential part of almost everything we do. And, as we've learned in previous briefings and hearings, in today's highly interconnected, digital world, the threat of cyberattacks to the reliability of electricity is ever present and growing.

One of our responsibilities on the Energy and Commerce Committee is to review, and where necessary, revise laws and policies that concern the reliable delivery of energy. This is part of the Committee's black letter jurisdiction, and it is something we take very seriously on both sides of the aisle, no matter which party is in the majority.

This morning's oversight hearing continues this important work. It focuses on the status of efforts to address cyberthreats to the electric grid. We will hear testimony from three of the key players for making sure the lights stay on: Department of Energy, the Federal Energy

Regulatory Commission, and the North American Electric Reliability Corporation, or NERC.

Each of these organizations has a role in supporting effective information sharing, technical assistance, standard setting, oversight of standards implementation, and sound engineering practices relating to the bulk power system. And I look forward to hearing updates from the witnesses, especially on coordination and sharing among the federal entities and industry.

Our past oversight has examined some of the work DOE is doing to carry out its broad energy emergency and cybersecurity responsibilities over the energy sector. This includes providing, supporting, and facilitating the technical assistance to the energy sector to help identify vulnerabilities and mitigate risks. I’ve seen some of this work at the National Labs, particularly at the Pacific Northwest National Laboratory, in Washington, and at the Idaho National Laboratory, which provide analytical tools, test beds, and other capabilities that are proving very helpful for industry.

We learned last year how deployment of new surveillance and information sharing tools, particularly in what is called the Cybersecurity Risk Information Sharing Program, or CRISP, have proven especially helpful in identifying systematic cyberattacks across the energy sector.

I would be interested to hear today from NERC and DOE how this approach is being expanded more broadly, especially as it relates to supply chain risks and operational technology systems – the switches and Supervisory Control and Data Acquisition (SCADA) system – embedded in the grid. We know that as more connected devices and smart grid technologies are added to the grid, the vulnerabilities will continue to grow.

Information sharing is central to strong cyber defenses. This is especially important as our energy systems become more interconnected. Republican Leader Upton has noted repeatedly how, because the nation’s pipeline systems are such an integral part of the electricity fuel supply system, harm to pipelines means potential harm to the supply of electricity.

We must think about pipelines as part of a larger energy system – rather than a piece of hardware or a simple mode of transportation. While pipelines fall under separate regulatory regimes, DOE must maintain visibility over pipelines to ensure the delivery of electricity to consumers. That is why this Committee has been pushing to codify

DOE’s emergency response role and strengthen the Department’s capabilities to monitor for cyberthreats and to provide technical assistance to industry.

It is also important to enhance coordination of response should attacks succeed at a large scale. Members on this panel have had the benefit of briefings over the past few years to understand emergency response exercises in the electric sector. An update on these exercises will be useful today.

As testimony this morning will underscore, the risks to our critical electric infrastructure from nation states and other bad actors is increasing. This means the technical assistance, the information sharing, and deployment of innovative technologies and best practices to get ahead of the threats is ever more urgent. We must be sure that our critical infrastructure protection standards are up to date and sufficiently flexible to meet the risks. We must be sure that we are providing our federal agencies the tools needed to serve the industry and the nation more effectively. We have a responsibility here and hearings like this will help us do our job.

Thank you. Mr. Chairman, and I yield back.