Welcome to today's hearing of the Energy and Commerce Committee's Subcommittee on Oversight and Investigations.

We depend on our electric infrastructure for many of the activities essential to our daily life: heating and cooling our homes, powering industrial operations, operating medical equipment, and treating our water supply.

Unfortunately, days—or even hours—without electricity can have devastating consequences as some of my constituents experienced firsthand last December when Southwest Virginia suffered from extremely low temperatures and some power outages and rolling blackouts.

Securing our electric infrastructure is an increasingly demanding and complicated challenge, given novel threats from foreign groups and governments and the increased complexity of our critical infrastructure. In May of 2021, a cyber-criminal group's ransomware attack struck the Colonial Pipeline Company and led to a proactive shutdown of that company's pipeline system which in turn caused fuel shortages on the East Coast.

Our foreign adversaries have also demonstrated an increasing interest in their ability to undermine our critical infrastructure and strengthening their cyber capabilities. According to the Director of National Intelligence, Russia will continue to focus on improving its ability to target critical infrastructure in the United States, and China is likely capable of cyber-attacks that could disrupt our infrastructure.

In fact, just last week, reports emerged that Chinese-based hackers have infiltrated emails accounts at the State Department and Department of Commerce.

The proliferation of so-called "internet-of-things" or smart devices, anything from your television to an electric car, raises new risks for our electric grid. The implications on grid security have not been fully fleshed out.

Additionally, last December, the Environmental Protection Agency published proposed greenhouse gas standards for fossil fuel-fired power plants, which could burden dependable resources such as coal and natural gas and force generation facilities offline, jeopardizing reliable baseload power.

I have joined many of my colleagues in fighting back against these rulemakings and will continue to demand answers regarding this aggressive rulemaking onslaught.

Further, last year, the Department of Energy proposed new energy efficiency standards for distribution transformers, which I believe would severely exacerbate already serious supply chain constraints for this equipment. This is terrible timing on the Department of Energy's part.

To combat this supply chain threat and potential danger to our grid, I am an original cosponsor of Congressman Hudson's legislation, the Protecting America's Distribution Transformer Supply Chain Act.

That bill prevents the Department of Energy from implementing new distribution transformer standards for five years.

Probing federal efforts to secure our critical infrastructure, exploring risks that need further attention, and identifying opportunities to enhance cooperation among stakeholders is an important task for this subcommittee.

To that end, on May 16th of this year, I convened a hearing to examine the work of three of our Sector-Specific Agencies in protecting their respective critical infrastructure sectors from cyber threats. At the hearing, Members of this Subcommittee questioned the Director of the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response on the Department's efforts to secure energy systems and coordinate with energy infrastructure operators to accomplish this shared goal. I hope we can build on that discussion today.

We have more infrastructure security experts with us today to share their knowledge with us.

First, we welcome Mr. Manny CAN-Cell of the Electric Information Sharing and Analysis Center, or E-ISAC. E-ISAC compiles and analyzes security data for the electric industry, coordinates incident management, and circulate mitigation strategies among stakeholders.

Also joining us is Mr. Sam Chanowski of the Idaho National Laboratory.

As part of the Department of Energy's national lab complex, Idaho National Laboratory hosts research and testing to strengthen the electric grid and critical infrastructure security, among other activities.

We also welcome the Honorable Bruce Walker, President and Chief Executive Officer of the Alliance for Critical Infrastructure Security and who formerly served as Assistant Secretary for Energy at the Department of Energy.

Finally, we are also joined by the Honorable Dr. Paul Stockton of Paul Stockton, LLC, who formerly served as Assistant Secretary of Defense for Homeland Defense

Our witnesses here with us today offer a wealth of experience in the cybersecurity, national security, and electric infrastructure fields, and we appreciate them sharing their expertise with us today.

Thank you, and I look forward to having a productive discussion.