CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

Opening Statement
Chairman Stephen F. Lynch
Subcommittee on National Security Hearing
"Securing the U.S. Electrical Grid"
July 27, 2021

Good afternoon, everyone. Before we begin, I would like to thank each of our witnesses for testifying before our Subcommittee today. I would also like to thank my colleagues who are participating at today's hearing both remotely and in-person.

If you have listened to the news this past year, there is a good chance you have heard about one of the many cyberattacks that targeted a high-profile technology company, research institution, energy pipeline, or even the federal government.

Today we will examine how this latest uptick in hacking attempts could affect a vital component of our critical infrastructure, and even U.S. national security: the electrical grid.

The electrical grid is the backbone of daily life in America: it provides energy to heat our homes, power our hospitals, and charge our smartphones. It is also a priority target for state and non-state cyber adversaries. A successful attack on the electric grid could have devastating consequences for U.S. national security and economic interests.

Last month, Secretary of Energy Jennifer Granholm confirmed that U.S. cyber adversaries have the tools and capabilities necessary to shut down our electrical grid. In a recent statement, the Department of Energy warned, "The United States faces a well-documented and increasing cyber threat from malicious actors seeking to disrupt the electricity Americans rely on to power our homes and businesses."

In response, President Biden has taken decisive, meaningful action since assuming office to strengthen our national cyber defenses and protect our critical infrastructure. For example, in April, President Biden announced a 100-day plan, led by the Department of Energy and the Cybersecurity and Infrastructure Security Agency, to strengthen the security and resilience of the U.S. electrical grid. And in May, President Biden issued an executive order that will modernize our national cybersecurity defenses and improve information-sharing between the U.S. government and the private sector, which is ultimately responsible for operating and securing the electrical grid.

I applaud President Biden for recognizing the urgency of this threat. However, significant vulnerabilities persist, and the Biden Administration should consider whether additional regulations or policy initiatives are needed to strengthen the cyber defenses and resilience of the electrical grid.

For example, as a growing number of networked consumer devices connect to electrical distribution systems, these devices create additional gateways that hackers can exploit to gain access to the grid. These vulnerabilities are exacerbated by the fact that federal cybersecurity standards do not currently apply to distribution systems and are instead only mandatory for certain generation and transmission systems. Even those mandatory reliability standards that apply to electric generation and transmission systems do not fully incorporate leading cybersecurity guidance from the National Institute of Standards and Technology.

In addition, many key components of the electrical grid are produced, or rely on parts produced, by international suppliers. This equipment is vulnerable to tampering or espionage by foreign actors. Some of this equipment, especially large power transformers, can take over a year to produce, transport, and install—even in an emergency—making the U.S. electrical grid heavily dependent on overseas manufacturing.

Last, but certainly not least, multiple federal agencies and state and local entities—each with its own role, responsibilities,

and authorities—are all tasked with protecting the electrical grid. This creates ample opportunity for bureaucratic stove-piping and can undermine incident response. To that end, I look forward to hearing from our witnesses about how they are working together and sharing information to ensure malign cyber actors cannot slip through any cracks.

With that, I would like to thank our witnesses for their service and for testifying before our Subcommittee today on this critically important issue, and I will now yield to the Ranking Member from Wisconsin, Mr. Grothman.

###

Contact: Emma Dulaney, Deputy Communications Director, (202) 226-5181