Chairman Manchin's opening remarks during a full committee hearing to examine the steps needed to address the cybersecurity vulnerabilities to the United States' energy infrastructure.

Introduction

- The committee will come to order.

- Before I turn to my opening statement about our hearing today, let me begin by noting that if we get a quorum of 7 members, we'll take a moment to adopt a resolution appointing members of our subcommittee.

- Now today we will be discussing the steps needed to address cybersecurity threats to the United States' energy infrastructure.

- In addition to energy resources being used as a geopolitical weapon against our friends and allies, our adversaries have increasingly begun using cyberattacks to infiltrate American infrastructure to disrupt our energy security and economy.

- The rapidly changing cyber threat landscape will require constant federal attention and strategic flexibility to ensure we are ahead of the curve and not caught off guard to the detriment of our national security, public health and safety, and economy.

- Our government has taken substantial steps in the past decade to improve federal coordination, increase funding for research and development, enhance intelligence dissemination, and build on existing public-private partnerships.

- I want to thank our witnesses for joining us today to contribute to this important discussion and provide input on additional actions Congress needs to take to strengthen our energy cybersecurity strategy.

Threat Environment

- Cyber threats can be attributed to individual bad actors, transnational organized crime, state-sponsored groups, and nations.

- The 2022 Annual Threat Assessment from the Office of the Director of National Intelligence assessed China as the broadest and most active cyber threat to the U.S. Government and private sector networks.

- In addition, the assessment identifies Russia as the top cyber threat that is specifically focused on targeting our critical infrastructure.

- Russia’s cyberattack that shut down Ukraine’s electricity grid in 2015 was a wake-up call to the possibility of large-scale cyberattacks on critical infrastructure like the electric grid.

- Putin's vicious aggression in Ukraine increased the likelihood that Russia will increasingly rely on extreme and dangerous tactics against Ukraine’s allies, such as using cyberattacks as retaliation for sending arms and aid to Ukraine.

- Domestically, our relevant agencies and industry have been on heightened alert.

United States Energy Infrastructure

- Cyber incidents impacting our domestic energy infrastructure pose a persistent threat, many of which we never hear about.

- However, some recent attacks have highlighted the severity of cyberattacks directed at our energy infrastructure.

- In 2021, the Colonial Pipeline ransomware attack forced the shutdown of the country’s most important fuel pipeline for nearly a week.

- Colonial delivers nearly half of the gasoline, jet fuel, and diesel to the East Coast—over 100 million gallons per day.

- The Department of Energy provided a stark assessment – if the pipeline had been down for a few more days, it would have resulted in diesel rationing, and chemical and refinery operations would have been suspended due to an inability to transport their production.

- Just last year, the Department of Justice charged four Russian government officials who used cyberattacks to target critical infrastructure companies from 2012 to 2018.

- They breached hundreds of energy companies worldwide, including a nuclear power plant in Kansas, intending to disrupt our global energy system.

- Moreover, there have been numerous reports of attempted cyberattacks on the U.S. electric grid and natural gas sites.

- Our energy system is rapidly evolving. Our aging grid is not designed to protect itself from modern cyberattacks and is transforming into a new network-connected environment.

- In addition to the electric grid, pipeline networks are becoming more dependent on internet-based control systems for their operations.

- As we improve our energy systems with remote and automated capabilities intended to make energy more reliable, this new connectivity raises the stakes for security intrusions.

- We must also consider the new distributed energy resources connecting to our grid.

- Americans are purchasing rooftop solar panels and electric vehicles at a rapid rate. These resources provide benefits to consumers, but present serious cybersecurity challenges to our grid.

- While experts are still determining the degree of risk, there is concern that these new resources can serve as additional "entry points" for cyber adversaries to target the grid and could have the possibility to cause major disruptions.

Federal Efforts

- As cyber-attacks on our energy systems have increased, our nation's national and energy security relies on steadfast commitment from our federal agencies and private partners.

- DOE is the Sector Risk Management Agency for the energy sector.

- This means DOE has the responsibility to coordinate information sharing, response operations, technology development and deployment, and other energy cybersecurity responsibilities across the federal government.

- In that role DOE works closely with FERC and NERC, which have jurisdiction over cybersecurity standards for electric generators and transmission, and the TSA, which has jurisdiction over pipeline cybersecurity.

- Yesterday, Senator Risch and I introduced the *ETAC [E-TACK] Establishment Act*, which establishes the Energy Treat Analysis Center at DOE.

- ETAC will serve as the energy sector's centralized hub in the federal government for cyber information sharing and threat response, and DOE will be able to better defend the U.S. energy sector against cyber threats and inform the industry of actionable steps they can take with their threat response.

- The creation of this center is critical to the energy security of our nation and I look forward to hearing more from DOE about their work on it.

- A cybersecurity incident has the ability to cripple our economy, and we must pay attention.

- We took action last Congress by providing $1.9 billion in the Infrastructure Investment and Jobs Act to shore up cybersecurity across the transportation, energy, and water sectors by supporting utilities and state and local governments. I am immensely proud of this work.

- In addition, the CHIPS and Science bill authorized $14.7 billion in funding for our National Labs, which lead our nation with their expertise in advancing the research and development of our cybersecurity capabilities.

- But more can be done. As Chair of this Committee and the Senate Armed Services Cybersecurity Subcommittee, I am very invested in the security of our energy infrastructure.

Conclusion

- We have gathered before us a group of experts in this field who I know can provide us with recommendations that we can turn into concrete, bipartisan legislative action.

- Cybersecurity and energy security impacts all of us and our constituents. We can and we must continue to take steps to empower our agencies and industry to effectively respond to these threats.

- With that, I will turn it over to Senator Barrasso for his opening remarks.

- Thank you, Senator Barrasso.

- I'd like to turn to our witnesses,

    - We will begin with Mr. Kumar

    - He will be followed by Mr. Lee

    - And finally, Mr. Swick

- Thank you all for joining us today,

- Mr. Kumar we'll begin with your opening remarks.

- Thank you, Mr. Kumar. We will now go to Mr. Lee.

- Thank you, Mr. Lee. And finally, Mr. Swick.

- Thank you, Mr. Swick. Thank you all again for being here with us, and for your testimony. We will now begin with questions.