Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Hearing on "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies"

May 16, 2023

Today, the Subcommittee continues its important bipartisan oversight of cybersecurity and protecting our nation's critical infrastructure from cyberattacks. Federal agencies within our Committee's jurisdiction and their partners in the private sector face serious cybersecurity threats to critical energy, water, and health systems. Major cyber incidents have repeatedly shown how harmful attacks on critical infrastructure can be to our nation.

We all remember the ransomware attack on the Colonial gas pipeline. The attack triggered panic buying that contributed to fuel shortages and higher gas prices across the East Coast and the South. At the end of last year, cyber criminals stole the electronic patient records of more than three million patients from a California hospital system. That breach exposed sensitive personal information, including patients' Social Security Numbers, test results and diagnoses, and prescription history. And then earlier this year, the personal health care information of Members and staff was stolen when DC Health Link was breached.

Cyber threats to critical energy, water, and health infrastructure are unfortunately becoming more common and attacks are more costly. In 2022, hundreds of cyberattacks cost health care organizations billions of dollars and made it harder for doctors and other health care providers from caring for patients for months afterwards.

Companies that own critical infrastructure face thousands of cyberattacks every year. While many of these attacks are unsuccessful thanks to the cyber defenses these companies have established, successful cyberattacks can have devastating consequences. During the early days of Russia's invasion of Ukraine, Russian hackers unsuccessfully targeted America's energy grid. Experts have said that this incident is the closest we have come to losing control of grid infrastructure and that the methods used represent an unprecedented threat.

That is why bipartisan efforts in this Committee are so important to bolster cybersecurity for critical infrastructure overseen by the Department of Energy (DOE), the Environmental Protection Agency (EPA), and the Department of Health and Human Services (HHS). We worked together on the bipartisan America's Water Infrastructure Act of 2018. This law requires water systems to complete risk assessments and develop emergency response plans that account for cybersecurity risks.

Despite these efforts, there are still gaps in the ability of federal agencies to prevent potential cyberattacks. In 2020, Russian hackers gained access to an update server at

SolarWinds, a software company serving critical infrastructure companies and federal agencies. For months, the attackers were able to use SolarWinds' systems to penetrate networks at hundreds of organizations and dozens of federal agencies. While the method of attack was not necessarily new, the scale and scope was unprecedented. It exposed vulnerabilities and cybersecurity gaps that put critical infrastructure at risk.

I strongly believe that DOE, EPA, and HHS are best equipped to handle internal and sector-relevant cybersecurity concerns. Much of our critical infrastructure relies on unique systems and specialized workforces. These agencies have the institutional knowledge and expertise to engage with their private-sector partners to address complex, sector-specific threats.

We must focus on giving these agencies the resources they need to fight constantly evolving threats. But the Republicans' Default on America Act threatens indiscriminate cuts to federal agencies overseeing infrastructure. I am concerned that it could seriously hamstring cybersecurity efforts at a time when we must be ramping up our defenses against cyber threats from criminals and foreign adversaries.

Federal agencies need tools that enable them to leverage sector-specific expertise and institutional knowledge to prevent and respond to cybersecurity concerns. With bipartisan congressional support, DOE, EPA, HHS, and other federal agencies can continue to develop more efficient and robust cybersecurity defenses while also partnering with the private sector to protect our critical infrastructure systems.

I hope to continue the Committee's important bipartisan work on this topic, and I look forward to hearing from our witnesses on the progress they've made and the challenges that remain.

Thank you, I yield back.