Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Oversight and Investigations Ranking Member Kathy Castor

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

May 16, 2023

Thank you, Mr. Chairman. I'm glad we're having this important hearing to get a better understanding from the agency experts as to the threats to critical infrastructure, how they are addressing those threats, and how we can support their efforts.

Every day, folks in my district and across the country count on being able to turn on their lights, have easy access to clean water, and ensure that they can receive confidential and life-sustaining medical treatment. Yet, the critical infrastructure that makes these things possible is increasingly under threat from criminals and foreign adversaries who carry out cyber attacks to steal people's personal information and disrupt our way of life.

So we must prepare, and protect critical infrastructure now from more common and sophisticated cyber attacks. They target not only the agencies that are here today but also the utilities, companies, and healthcare providers throughout the sectors they oversee. Every hospital and utility is a target for bad actors seeking to profit from sensitive information or undermine our national security.

Criminal networks have targeted hospitals and public health agencies in ransomware attacks because they know that these organizations store our neighbors' most personal information. I want to do all I can to protect my neighbors and the hospitals and health systems that serve them.

Foreign adversaries like Russia have used cyber attacks to steal information from hundreds of federal agencies and critical infrastructure organizations. Just last year at the start of Putin's invasion of Ukraine, Russian hackers tried to take control of energy facilities in the United States. While those hackers were ultimately thwarted by the Department of Energy and its federal and sector partners, it demonstrates the seriousness of cyber threats and the risks that they pose.

Many critical infrastructure organizations can take steps to prepare for and prevent cyber attacks. In doing so, the impact of an attack can be mitigated, but it takes an understanding of sector-specific cybersecurity threats to ensure that finite resources are spent on the most effective measures.

That is why the work that the Department of Energy, Environmental Protection Agency, and Department of Health and Human Services do to develop cybersecurity best practices and

educate their sector partners is so important. These agencies have the expertise necessary to identify sector- and sometimes facility-specific cyber threats and can use their existing regulatory relationships to make sure that countermeasures reach the organizations that need them the most.

As we tackle the rising costs and risks of the climate crisis, cybersecurity will only become more important. Clean energy resources will help us reduce climate pollution, while new technologies that replace legacy systems can help existing power plants operate more efficiently, but new technologies can also give hackers angles to attack our energy infrastructure.

We need to make sure that energy and other critical infrastructure are well protected so that we can benefit from technological innovation.

Agencies already are taking steps to address foreseeable cyber threats and Congress can and should continue to support their efforts in a bipartisan manner. By listening and learning from our experts, Congress can make sure agencies have the tools that they need to keep our neighbors safe, counter cyber threats and protect critical infrastructure.

I look forward to hearing from our witnesses about their important cybersecurity work they do and see how Congress can be helpful in supporting the most effective cybersecurity tools.

Thank you, I yield back.