Opening Statement for Chair Cathy McMorris Rodgers
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
"Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies"
May 16, 2023

Thank you, Chair Griffith

EMERGING THREATS AND GROWING VULNERABILITIES

Today, we are here to learn more about cyberattacks that threaten the essential services and products that we, as a nation, need to survive.

Attacks that could deprive us of access to emergency services; food and water; and the ability to communicate with one another.

As Chair Griffith described, our critical infrastructure is essential to the security of our nation, our economic prosperity, and our way of life.

We depend on critical infrastructure to power our homes, ensure we can get to work, call for help in an emergency, supply us with clean water, and produce our food.

With technological advances, this network has become increasingly more complex and interconnected. However, as our physical infrastructure and digital systems become more intricately intertwined, new opportunities bring with them new challenges.

Bad actors, whether criminal organizations or foreign adversaries, have demonstrated a growing interest in launching cyberattacks on critical infrastructure. And unfortunately, many have demonstrated that they have the capability to do so.

For example, the number of yearly cyberattacks on United States hospitals reportedly doubled between 2016 and 2021.

Hospitals have increasingly become targets for ransomware gangs, which assume control of online networks and then demand a ransom to unlock them.

This means care and treatments are delayed when lives are on the line.

Additionally, in 2021, a hacker altered the chemical levels in the water supply at a water treatment facility in Florida.

Last June, another report concluded that 89% of electricity, oil & gas, and manufacturing firms experienced cyberattacks affecting production and energy supply over the previous twelve months.

SECTOR RISK MANAGEMENT AGENCY EXPERTISE

Securing our critical infrastructure from cyber threats and responding quickly to minimize and contain interruptions to these services will require the unique skills and resources of nearly all of our federal agencies.

Each of our Sector Risk Management Agencies possess specialized knowledge and expertise to help them identify new and evolving cyber threats to its particular infrastructure sector.

Through their experiences regulating and communicating with critical infrastructure owners and operators, these agencies have gained extensive knowledge of the utilities, industries, and facilities that comprise each sector.

For example, the Department of Health and Human Services is uniquely well-positioned to respond to emerging threats to our hospital systems' online record systems because HHS is the agency already in direct communications with the health care sector.

CROSS-SECTOR PARTNERSHIPS

Similarly, we plan to explore whether our Sector Risk Management Agencies effectively partner with the private entities, utilities, and non-federal government entities that make up the critical infrastructure network.

Many of these entities, particularly small businesses, local governments, or small utilities may not have the resources to address the constantly shifting cyberthreats they face and can benefit greatly from the resources and technical assistance our Sector Risk Management Agencies can provide.

Our federal agencies are also well positioned to provide leadership, coordinate efforts, and information sharing among members of each critical infrastructure sector.

Much of our critical infrastructure is owned or operated by the private sector, so we hope to learn more about our Sector Risk Management Agencies' strategies for forging partnerships across relevant industries.

We hope to learn more about how these agencies listen to their non-Federal partners and receive their feedback to ensure federal cybersecurity programs appropriately serve those they seek to protect.

In the same vein, in carrying out their cybersecurity responsibilities, federal agencies should incorporate the expertise they gather from their regulated entities and other non-Federal partners to inform their efforts.

As we have discussed, many of our critical infrastructure sectors are heavily intertwined and rely on each other to function properly.

As such, we hope to learn more about our Sector Risk Management Agencies' efforts to coordinate with each other and share expertise, lessons learned, and best practices.

CONCLUSION

Cyber threats to our critical infrastructure present a serious risk to our national security.

We can be prepared for these threats if we effectively harness the expertise and creativity of our federal agencies, non-federal governments, utilities, and industry.

Again, I thank our witnesses for sharing their perspectives today, and I look forward to the discussion.