Committee on Energy and Commerce

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

Hearing on "Protecting Clean American Energy Production and Jobs by Stopping EPA's Overreach"

January 31, 2024

I wanted to begin by welcoming our new Environment Subcommittee Chair, Representative Carter. I am pleased we are beginning your tenure with a bipartisan issue, and I hope that we can continue that approach with other environmental issues where bipartisan consensus might be possible. I look forward to working with you, and congratulations on your new leadership role.

Today this Subcommittee continues our important bipartisan oversight of cybersecurity and protecting our nation's critical infrastructure from cyberattacks. Specifically, we will take a closer examination of the water sector and how we can best equip water systems and the Environmental Protection Agency (EPA) with the resources and tools needed to assess and mitigate risks from cyber attackers.

Major cyberattacks have become more frequent and more sophisticated, putting our nation's critical infrastructure at risk. This is especially true for cyber incidents targeting our drinking water and wastewater systems. In fact, the water sector is classified as a National Critical Function because a disruption to water systems can have devastating impacts on the health, security, and safety of communities. A disruption could also greatly impair the various other critical infrastructure sectors that depend on water – such as the energy and health care sectors.

Cyber attackers have targeted U.S. water systems of every size and in every corner of our country. An attack on a Maine-based water utility in 2021 used ransomware to target internet-facing operational technology, forcing the utility to revert to manual control of critical processes. Later that year, an attack on a California-based water utility utilized ransomware that went undetected for a month. And more recently, an Iran-linked group called "CyberAv3ngers" targeted Israeli-made equipment at water facilities across several states, including Pennsylvania and Texas.

Much of our nation's critical infrastructure relies on unique systems and specialized workforces – and the water sector is no exception. There are over 150,000 public water systems across the nation that range in size from serving less than 500 customers to millions. Over 90 percent of water systems are small, which can bring unique managerial, financial, and operational challenges as they strive to deliver safe drinking water to their customers. Lack of capacity and resources at these water systems adds further challenges.

That is why our Committee's bipartisan efforts to bolster cybersecurity for the water sector are so important. Most recently, 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 risks – including cybersecurity. This was an important step but there are still gaps in the ability of federal agencies and water systems to prevent potential cyberattacks. I hope that we can continue our history of bipartisan cooperation to assess and address these gaps as quickly as possible.

I strongly believe that EPA is best equipped to handle cybersecurity concerns for the water sector. EPA has the institutional knowledge and expertise to engage with water systems and other federal partners to address complex, sector-specific threats. Currently, EPA provides technical assistance, education, and resources to help water systems bolster cyber protections. And last Congress, we authorized and reauthorized several grant programs to help water systems address their vulnerabilities as part of the Bipartisan Infrastructure Law.

This Committee has to ensure that EPA has the necessary tools and can leverage sector-specific expertise and institutional knowledge to adequately prevent and respond to cybersecurity concerns. With bipartisan congressional support, EPA can continue to develop more efficient and robust cybersecurity defenses while also partnering with the private sector and other federal agencies to protect our critical infrastructure systems.

Finally, I would like to submit a letter from Representative DeLuzio of Pennsylvania into the record. The water utility in his district was one of the systems targeted by the Iran-backed cyber group, and he wanted to share his experience about that incident with the Committee.

And with that, I yield back the balance of my time.