Opening Remarks of Ranking Member Whitehouse: *"Identifying and Addressing Cybersecurity Challenges to Protect America's Water Infrastructure."*

Thank you, Chair Capito, for convening us on another important topic and to the witnesses for taking time to be here.

Cybercrime and cyberwarfare are realities of the 21st century and have been for decades. In 2010, I served on the Intelligence Committee Cyber Task Force where we spent six months investigating cybersecurity threats to our country. The water sector has modestly improved information sharing and coordination between the EPA and the Cybersecurity and Infrastructure Security Agency, and non-profits and water sector trade groups have increased public awareness of cyber threats. This, however, is wholly insufficient. Meanwhile, bad actors continue to enhance their capabilities and evolve the nature of their attacks.

State-sponsored and state-aligned bad actors linked to countries like Russia, China, Iran, and North Korea have been increasingly relentless in their attacks on American facilities. They have stolen sensitive information, scrambled networks, extorted ransoms, and disrupted sectors ranging from health care to drinking water.

There are nearly 170,000 water systems across our country. As these systems modernize, they incorporate technology that is more efficient, yet more vulnerable to cyberattacks. According to GAO, many of these facilities have already faced digital breaches, but without more incident reports it is impossible to know the full scale of the threat we face.

Since 2023, Russian, Iranian, and Chinese hackers have successfully attacked small municipal water systems in Texas, Pennsylvania, and Massachusetts, and have tested the security capabilities of countless other systems. Over the past six years, Rhode Island municipal facilities, including a large wastewater utility, have experienced at least six cyberattacks, collectively resulting in hundreds of thousands of dollars in losses. These are just the incidents that have been reported.

All water utilities without adequate cyber security are at risk, regardless of size. While none of the previous attacks on the water sector have caused major service disruptions, they all cost time and money. A cyberattack that incapacitated even one water facility would not only be disastrous for the people affected, it would spread fear across the country.

According to an EPA survey, less than 25 percent of our water and wastewater utilities perform annual cyber risk assessments. Just imagine the consequences of a coordinated nationwide hit. Clearly, we are not ready.

The Trump administration has forced out thousands of federal cybersecurity experts, cut funding to research and readiness programs, and crippled our relationships with key international intelligence partners. We need to strengthen our national cybersecurity capabilities, not weaken them, and water utilities need more knowledge-sharing, not less. We can change that now.

Even when water utilities understand the risk and solutions, updating cybersecurity measures is often deferred in favor of maintaining service levels to ratepayers. To meet the challenges of the 21st century, we must repair and replace outdated infrastructure while *also* updating and maintaining our cybersecurity capabilities. This is not an either or.

To start addressing our nation's massive water infrastructure investment deficit, the Infrastructure Investment and Jobs Act provided more than $50 billion, with some expanded eligibility for cybersecurity projects.

This was a good start, but it was not nearly enough. I look forward to discussing how this Committee can expand EPA's current authority and can help update physical and digital infrastructure across the country to keep water safe, available, and affordable.