Thank you Chairman Carper, Ranking Member Capito, and the distinguished members of the Committee for the opportunity to speak with you today. I am pleased to be here along with my Cyberspace Solarium Commission co-Chair, Congressman Mike Gallagher, to talk about how we might improve the cybersecurity of one of our nation's most critical sectors.

Congressman Gallagher paints a disturbing picture. Threatened by criminals and nation-state adversaries alike, as this Committee is aware, our water sector is at risk. Less than a decade ago, its disruption through cyber means seemed like science fiction, but in the last several years we have witnessed widespread and impactful cyber attacks on our critical water infrastructure from Florida to California. The time is now to explore solutions to the challenges we face in securing our water systems.

As the U.S. Cyberspace Solarium Commission details in its report, pushing back against bad cyber behavior is both an offensive and a defensive activity. On the offensive side, we possess the world's most capable cyber operators in our Department of Defense and National Security Agency. We must continue to enable these entities to defend forward against foreign threats and disrupt our adversaries at the source. On this front, the United States is making effective investments.

However, we have chronically underinvested in cyber defense for decades. The necessary investment can take many forms. We need to build capacity and provide better advice to less mature organizations, exchange better information with more mature organizations, and build a more integrated relationship between our largest, most mature—and often, most at risk—partners in the private sector and the federal government. This applies across the board with our sixteen critical infrastructure sectors, but is particularly salient in the context of the water sector.

Defense starts at the local level, where many smaller rural water utilities struggle to identify, assess, understand, and ultimately mitigate cyber risk. The Federal government has a duty to help these entities manage such risk. Two specific programs stick out as relevant in this context. First, the circuit rider program provides hands-on technical assistance to water system operators on a variety of issues. This program could be expanded to incorporate technical cybersecurity assistance. Second, the work of National Laboratories to identify cybersecurity vulnerabilities in the operational technology environments of the energy sector should serve as the groundwork for similar efforts and trickle out to other sectors, including the water sector.

Moving up the chain, mid-sized and more mature entities in the sector thirst for more knowledge and information regarding the threats that they and their counterparts face. In most sectors, Information Sharing and Analysis Centers (ISACs) serve as coordinating bodies to facilitate the sharing of cybersecurity information among entities in a given sector. The waterISAC provides free services to the water and wastewater sector but is under-resourced. An augmentation of their budget through a federal grant would allow them to expand their services to enhance the overall cyber readiness and resilience of the sector through risk assessments, advisory support, incident tracking and analysis, and training and sector-wide exercises.

Finally, at the top of the chain, the most mature and riskiest entities need to be brought closer to the Federal government. Reinvigorating this relationship should take two forms. First, we as a Federal

government must do a better job of assessing national risk and working with the entities that own and operate infrastructure that, if disrupted, could produce catastrophic consequences for our national security, economic continuity, or societal resilience. To do this, the U.S. Cyberspace Solarium Commission recommended the passage of legislation tasking the Department of Homeland Security with working with relevant sector risk management agencies to identify systemically important critical infrastructure and build more robust relationships with these entities, providing them with benefits—like enhanced intelligence sharing—and holding them to account for their cyber hygiene. Second, we must do more to ensure that mature companies are able to share with and receive information from the Federal government in real time. The creation of a cloud-based Joint Collaborative Environment would supply the Federal government and critical infrastructure owners and operators with a common, interoperable virtual environment to share and fuse threat information, insight, and other relevant data, allowing the federal government to give real-time warning of incoming threats.

These are important steps that we, as Congress, can take in the short-term to build greater cyber resilience in the water sector. In the longer term, we must consider how best to equip responsible Federal agencies, including the Environmental Protection Agency, with the resourcing and investment to set and normalize standards across the sector. Holding entities to a higher cybersecurity standard is, and will continue to be, crucial for ensuring that both systemically important critical infrastructure and the rest of the sector are fully prepared to defend the nation's water supply from the pressing threats that Congressman Gallagher eloquently described.

Thank you again to Chairman Carper, Ranking Member Capito, and the members of this Committee for the opportunity to speak with you today about this crucial issue. I look forward to working with all of you to improve the cybersecurity and resilience of our nation's critical water infrastructure.