Thank you Chairman Carper, Ranking Member Capito, and distinguished members of the Committee for the opportunity to speak with you today. I appreciate the chance to appear along with my U.S. Cyberspace Solarium Commission co-Chair, Senator Angus King, to talk about the importance of securing our nation's water supply from cyberattacks.

The U.S. Cyberspace Solarium Commission was authorized through the National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."[1] In the course of this work, we paid special attention to our national critical infrastructure and the importance of securing that infrastructure from both criminal and nation-state cyber threats.

The sixteen critical infrastructure sectors are not equally equipped when it comes to cybersecurity: There are leaders—like the financial services sector—and there are laggers. Despite the importance of our water systems, the water and wastewater infrastructure sector lags behind many of its peers, posing a risk to our public health and safety. In the report we submitted to Congress in March of 2020, the Commission concluded that "water utilities remain largely ill-prepared to defend their networks from cyber-enabled disruption."[2] As we've continued our work on improving the nation's cybersecurity, bolstering the ability of the water sector to detect, prevent, and withstand cyberattacks has emerged as a crucial priority.

Though 55 percent of utilities responding to a survey conducted by the Water Sector Coordinating Council rated cybersecurity as a high or top priority,[3] the overall cybersecurity of our water sector remains immature. A 2016 National Infrastructure Advisory Council report highlighted the "wide disparity" in the technical capabilities and resources of water utilities across the country:[4] Many of our nation's nearly 70,000 community water and wastewater systems[5] are small, publicly owned assets that are not equipped to deal with nation-state threats.[6] And the National Infrastructure Advisory Council has described federal support for the resilience of the water sector as "fragmented and weak."[7]

Municipalities have benefited greatly from the enhanced efficiency and quality brought by automated and remote systems for treating water supplies, but those same systems introduce new risks when not properly secured. As can often happen when budgets are tight and must be balanced, investments in security can fall by the wayside. The Water Sector Coordinating Council reports that 38 percent of utilities dedicate less than 1 percent of their budget to the cybersecurity of information technology, and 44.8 percent

---

[1] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (2018), https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf.
[2] U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission* (March 2020), 62, https://www.solarium.gov/report.
[3] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity 2021 State of the Sector* (June 2021), 18, https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf.
[4] National Infrastructure Advisory Council, *Water Sector Resilience: Final Report and Recommendations* (June 2016), 4, https://www.cisa.gov/sites/default/files/publications/niac-water-resilience-final-report-508.pdf.
[5] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity,* 3.
[6] National Infrastructure Advisory Council, *Water Sector Resilience*, 36-37.
[7] National Infrastructure Advisory Council, *Water Sector Resilience*, 97.

allocate less than 1 percent of their budget to the cybersecurity of operational technology.[8] Insufficient security investment leaves the water sector vulnerable to nation-state, criminal adversaries, and insider threats—disgruntled employees or former employees with specific knowledge of how to disrupt a utility's information technology or operational technology systems. Against these threats, the water sector faces challenges ranging from maintaining awareness of the threats to assessing risks to identifying and remediating vulnerabilities.[9] A shortage of qualified cybersecurity professionals across the globe compounds the problem,[10] making it difficult for resource-strapped organizations to attract and retain the talent necessary to protect our drinking water and public health systems.

Earlier this year, the city of Oldsmar, Florida, suffered a cyberattack in which malicious actors attempted to change the level of lye in the city's drinking water.[11] Though the attack was quickly detected and stopped, the situation could have been disastrous. In another incident, a malicious cyber actor compromised a California water treatment plant, deleting crucial programs meant to treat drinking water.[12] And in April, federal prosecutors unsealed a grand jury indictment of a former employee of a Kansas water utility who remotely tampered with the utility's cleaning and disinfecting procedures.[13] It was through sheer luck that none of these incidents affected customers.

A more sophisticated adversary could impact the safety of thousands of Americans through a cyberattack on our water supply. Beyond the direct impact to drinking water, a cyberattack affecting the water supply could have cascading impacts for other critical infrastructure sectors that rely on clean and safe water to function properly: That's why it's considered a lifeline sector.[14] These incidents underscore the importance of protecting our water systems and the need for more coordinated, consistent federal action to ensure that water utilities have the people, processes, and technology necessary to protect our public health and safety. Investment in the sector's cybersecurity must match the importance of the sector to our national security, economy, public health, and safety.

Thank you again to Chairman Carper, Ranking Member Capito, and members of the committee, for the opportunity to discuss this pressing issue with you today. We appreciate your attention to the matter, and with that, I would like to turn it over to my Cyberspace Solarium Commission co-Chair, Senator King.

---

[8] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity*, 8.
[9] Water Sector Coordinating Council, *Water and Wastewater Systems Cybersecurity*, 10.
[10] International Information System Security Certification Consortium, *Cybersecurity Professionals Stand Up to a Pandemic: (ISC)² Cybersecurity Workforce Study, 2020* (2020), 16, https://www.isc2.org/Research/Workforce-Study#.
[11] Peter Elkind and Jack Gillum, *America's Drinking Water Is Surprisingly Easy to Poison* (March 17, 2020), https://www.propublica.org/article/hacking-water-systems.
[12] Kevin Collier, *50,000 security disasters waiting to happen: The problem of America's water supplies*. NBC News (June 17, 2021), https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206.
[13] U.S. Department of Justice, U.S. Attorney's Office for the District of Kansas, *Indictment: Kansas Man Indicted for Tampering With a Public Water System* (March 31, 2021), https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system.
[14] National Infrastructure Advisory Council, *Water Sector Resilience*, 19.