

Below is the opening statement of Chairman Shelley Moore Capito (R-W.Va.) as delivered.

"Today we will examine the challenges facing drinking water and wastewater systems to install, implement and maintain adequate cybersecurity, as well as try to identify opportunities to address these challenges through new legislation.

"First, I want to thank our excellent panel of witnesses for making the trip to D.C. to share their perspectives on this important topic. Your work to enhance the resilience of our water and wastewater systems is incredibly important to Americans' health and daily lives.

"There are approximately—this number is stunning, really—170,000 water and wastewater utilities across the country. These utilities fill a vital role in ensuring that communities across the country have access to safe and reliable water and sanitation services.

"I know in the audience, we have several of our water system utility folks here. So, I'll shout out to my fellow West Virginians.

"Accessible and reliable water and wastewater services are essential to protect public health and provide fundamental services to our constituents. These services can also be a foundational basis for a strong economy and a strong America.

"Because of the important role our water systems play in our country they are unfortunately a target for bad actors. Over the last several years, we have seen a broad trend of entities linked to our geopolitical adversaries, such as Iran, China and Russia, using cyberattacks to target our critical water infrastructure.

"Cyberattacks on water utilities may take various forms. For example, ransomware attacks can compromise business or customer information. Attackers can also gain access and then manipulate a system's operational technology, disrupting the treatment or distribution of water or altering the levels of chemicals to potentially dangerous amounts.

"Either way, a successful attack that disrupts safe and reliable water or sanitation services or exposes sensitive customer data could be debilitating for impacted communities. These threats must be acknowledged and challenged, particularly as technological advances, such as AI, increase the speed and efficiency of these attacks.

"The rise in cyberattacks is occurring at the same time as our water and wastewater systems deploy new digital control technologies—I've seen some of them myself—systems that allow utilities to operate more effectively and effectively.

"As we look to upgrade and modernize our water systems in the face of these threats, it is more urgent for our utilities, federal agencies and water sector and cybersecurity experts to work together to increase that system resiliency.

"Increasing water system resiliency requires us to take a clear-eyed look at the many challenges and shortcomings that our utilities are facing:

- *Legacy systems are difficult to maintain and update;*
- *Workforce shortages limit in-house expertise; and*
- *Fulfilling basic cybersecurity hygiene practices requires consistent monitoring and communication.*

"For instance, in 2024 the Environmental Protection Agency identified instances where some water systems utilized a single login for all their employees, failed to change default passwords or did not curtail the ability of former employees to access the systems.

"While we work to improve the resiliency of our critical infrastructure from cyberattacks, solutions to address cybersecurity must be deliberate and tailored to

reflect the challenges faced by utilities of different sizes and locations. A one-size-fits-all mandate from the federal government will likely be overly burdensome and unworkable, particularly for our smaller systems, and can hinder utilities' ability to take achievable steps towards meaningful progress.

"Water and wastewater systems across our nation are already grappling with how to prioritize limited resources while meeting federal and state requirements under the Clean Water Act and Safe Drinking Water Act. Costly requirements can distract from the core mission of providing safe, reliable and affordable services to the American people.

"In addressing these cyber challenges, we must strike the right balance between the role of federal agencies and empowering local utilities to address their challenges and improve their cybersecurity at their own facilities. Due to the constantly evolving technological environment that we live in, addressing this challenge will require innovative solutions that enable utilities to adapt and respond to quickly changing circumstances.

"Building and maintaining resilience against cyber threats is not a one-and-done event – it is ongoing and ever-evolving. We should not rely on one specific technological advancement as the silver bullet solution or have blinders on when it comes to envisioning or preparing to address potential threats.

"I look forward the discussion today, learning how we can be better partners with our water utilities to identify cybersecurity threats and provide a flexible toolkit going forward."

# # #