Chair Earl L. “Buddy” Carter
Opening Statement—Subcommittee on Environment, Manufacturing, and Critical Materials: “Ensuring the Cybersecurity of America’s Drinking Water Systems”
January 31, 2024

As prepared for delivery

Before diving into today’s very important hearing, I’d like to take a moment to thank Rep. Bill Johnson for his leadership of the Environment, Manufacturing, and Critical Materials Subcommittee over the course of this Congress.

He leaves large shoes to fill, and I’d like to recognize his incredible work, especially on behalf his constituents in Ohio after the tragic events in East Palestine.

I am honored to follow his example and thank Chair Rogers for entrusting me with this new role.

As you all know, I represent the entire coast of Georgia, and I believe Georgia’s First Congressional District offers a unique perspective on the issues before this subcommittee.

We have abundant natural beauty that people come from around the world to see.

But it co-exists with a growing manufacturing base, including the mining and production of the critical materials necessary for our modern day of life.

I believe it is an excellent example of how we can protect our environment and human health while pursuing economic growth and prosperity that our constituents deserve.

I look forward to working with all the members of this Subcommittee on the important issues before us, like the one we are here to discuss today.

Water is the most essential compound on Earth.

Without clean supplies of potable water and systems to treat wastewater, our lives, our economy, and our communities would cease.

We know this and so do our adversaries.

China, Russia, Iran, and their proxies are constantly looking for ways to disrupt our critical infrastructure. Recent cybersecurity attacks on the water sector by Iranian hackers reminded us of this.

Luckily, these attacks did not impact the safety of our water supplies.

We must learn from these attacks and enhance the cybersecurity of our water sector assets. There are just under 50,000 community water systems and more than 16,000 publicly owned wastewater treatment systems in the United States.

Today, we will hear testimony from organizations representing all sizes and demographics of our country's water infrastructure. We'll also hear from the State agencies that have a front row seat to their work and help these utilities fulfill their essential mission.

As a former Mayor, City Council Member, and Planning Commission Member of a small, rural community, I understand the constraints facing many of our country's water systems and the collaboration that must be fostered to help them achieve their mission.

The water sector frequently operates on legacy technology systems, and small systems regularly lack the financial resources to hire cybersecurity staff.

Water utilities are also facing generational challenges.

The average age of a water system operator in the United States is 57 years old. These are individuals who did not grow up using computers and operating cybersecurity systems.

Because of these circumstances, we must meet these systems and their operators where they are and build on the cybersecurity efforts already occurring in the sector.

Big American companies are working with non-profits to pilot cybersecurity programs to coach operators on cyber hygiene practices to protect these systems.

The Water Information Sharing and Analysis Center, a non-profit managed by the water sector, serves over 3,000 water personnel and provides essential two-way communication between the sector and their government partners on cyber threats.

Rather than responding to these cybersecurity threats with one-size-fits-all regulatory standards that are costly and require and assume a level of technological sophistication to operate and maintain...

We must focus on ways to increase cybersecurity collaboration within the water sector, and opportunities for the Environmental Protection Agency and Department of Homeland Security to work jointly with these systems.

The water sector is a willing partner in this endeavor, and why wouldn't they be.

Water systems have an inherent interest in defending themselves from cyber threats and protecting the safety of the water for their customers. They do not need Washington agencies to remind them of this.

What they need is the technical knowledge and resources that help them protect themselves.

Cyber threats are not disappearing, and no amount of regulation, resources, or technical expertise can fully remove the threat.

However, by meeting the sector where it is and fostering an environment of collaboration, the sector’s cybersecurity resilience can be greatly enhanced.

I look forward to hearing from our witnesses about the diversity of our nation’s water systems and opportunities to enhance the cybersecurity of the sector.

Thank you for participating in today’s hearing.