U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Opening Statement

Environment Subcommittee Ranking Member Gabe Amo (D-RI)

Environment Subcommittee Hearing:

"Research-Driven Resilience:
Applying Science to Secure U.S. Water Systems from Cyber Threats"

May 21, 2026

Chair Franklin, thank you for holding this hearing, and thank you to our witnesses for joining us today.

Every American depends on safe and reliable water. It powers our hospitals, our schools, our military installations, and our homes. Our nation's 324 million citizens are served by nearly 170,000 public water systems.

Yet, the systems we depend on every day are increasingly vulnerable. Right now, foreign adversaries, ransomware gangs, and criminal networks are seeking to exploit weaknesses in our water infrastructure. The idea that Iran, China, or Russia could shut off or poison our drinking water sounds like a plot from a horror movie – but unfortunately, it's reality.

Our systems are being targeted not because they're wealthy, but because they're vulnerable. And cyberattacks against water systems have increased tenfold over the past few years.

In Rhode Island, a wastewater treatment facility in Narragansett Bay was hit with a ransomware attack in 2022. Operators reportedly were forced to pay $250,000 to regain access to their computer systems. Luckily, the attack did not disrupt wastewater collection or treatment services. But that money could have gone toward upgrading infrastructure, hiring staff, or keeping Rhode Islanders safe. And next time, we might not be so lucky.

If these systems go down, or worse, are manipulated, the consequences aren't just digital. They're physical. They're dangerous.

Malicious actors target water systems because they're vulnerable and because they know communities will be forced to pay. And if they don't, this isn't just a cyber issue; it's a threat to clean drinking water and public safety.

This is the challenge before us today.

This isn't just a technology problem. We already know how to defend these systems. The problem is implementing best practices and resources. Too many utilities are running on aging infrastructure, with limited-to-no cybersecurity staff, and outdated operational and information technology systems, while trying to defend against sophisticated threats. We're asking local water operators to be IT experts, cyber experts, and public health guardians all at once. That's not realistic. And it's why the federal government has to step up.

As the Sector Risk Management Agency, the Environmental Protection Agency is supposed to lead here. They are responsible for coordinating cybersecurity support, guidance, and risk management efforts. But it is severely understaffed, under-resourced, and stretched thin to fully meet this growing threat.

The Government Accountability Office has been clear: we are not meeting the scale of this threat, saying the EPA has gaps quote "to assess and support the water sector consistent with the scope and scale of the critical infrastructure challenges the sector faces."

So the questions for this hearing is simple:

> How do we ensure EPA has the personnel, resources, and authority to support utilities facing these threats?
>
> How do we help smaller and rural systems before vulnerability becomes a crisis?
>
> And how do we build a workforce capable of protecting our water infrastructure?

Because water infrastructure isn't just pipes and pumps anymore. It's public health. It's economic stability. It's national security. And we need to treat it that way.

I yield back.