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

Ranking Member Zoe Lofgren (D-CA)

Environment Subcommittee Hearing:

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

May 21, 2026

Thank you, Chairman Franklin and Ranking Member Amo for convening today's hearing.

This hearing is an opportunity for us to better understand the challenges local communities face in securing our water systems from cyber-attacks, and how science and technology can potentially address some of those challenges. Thank you to the witnesses for appearing today to share your expertise.

Access to clean water and functioning wastewater systems is a privilege most have us have long taken for granted in this country. When things work the way they are supposed to, we don't think about everything and everyone that makes it work. But our country's water infrastructure is aging and at risk on multiple fronts. If we do not act now to address those risks, widespread water insecurity for Americans could become a reality.

Today's hearing is focused on just one of those risks. The number and severity of cyberattacks against our drinking water systems, treatment plants, and wastewater systems are steadily increasing. It should worry us all that EPA has found that over 70% of the water systems the agency has inspected since 2023 do not meet basic security practices. If any of these cyberattacks become successful, the consequences could be dire. Disruption of water systems, at minimum, could lead to a health crisis and economic uncertainty.

These risks are only being compounded with the advancements in AI and the evolving methods that are accessible to malicious actors. Our aging infrastructure, especially in rural communities, is under-resourced and falling behind in becoming cyber resilient. This lag is making our water systems ever more susceptible to threats from malicious hackers and foreign adversaries.

In recent years, there have been several reports of hackers accessing water treatment plants across the country, attempting to poison the water, gain financial leverage, or prove their ability to infiltrate the systems. A 2024 cyber attack was directed at the largest water and wastewater utility in the country that services several states including California. There have been many more reports of these attacks on smaller facilities.

In my district, for example, we have a large and well-resourced water utility in the San Jose Water Company. They are well positioned to be a leader on water security and have been featured as a case study by the Water Information Sharing and Analysis Center. But my district spans a large area of rural, central California, with several less-resourced, smaller water utilities. Both the smaller and larger water utilities support many tech company facilities in Silicon Valley, making them a target for national security threats from foreign adversaries.

However, this situation is not unique to Central Valley. These threats are only being exacerbated by a change we are seeing in our country today. Large corporations are decentralizing their businesses from larger urban areas to more rural regions, as we build data centers and new manufacturing facilities across the country.

The intelligence community has pointed to water infrastructure being a major weakness in cyberwarfare. State-sponsored criminals are targeting facilities that support major manufacturing, data centers, or military facilities in an attempt to destabilize supply chains and cripple the central nervous system of information systems and networks. Fortunately, they have not yet been successful in any significant disruptions.

No matter how much a utility spends to defend itself, they are simply not going to have the same resources to bring to bear that nation states have. Therefore, this is a national security issue that requires a federal response.

So how do we go about addressing the water infrastructure cybersecurity weaknesses? What would an appropriately funded and resourced EPA be able to accomplish in supporting the thousands of water systems across the nation?

I look forward to investigating these questions and learning more about what we can do to make our water infrastructure better equipped to deal with cyber-attacks.

I yield back.