



Lauryn Williams - Written Testimony

New York State Senate Public Hearing on Water Security and Preparedness

October 1, 2026

Thank you, Senator Martinez, Senator Bottcher, Senator Ryan and members of the committees, for the invitation to provide testimony today. I am Lauryn Williams, and I serve as deputy director and senior fellow in the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS). CSIS is based in Washington, D.C. and is widely recognized as the leading U.S. national security think tank. My program's research agenda focuses on cybersecurity, and other cutting-edge technologies including AI, telecommunications, satellite networks and quantum through the lens of geopolitical competition with China as well as partnerships with our friends and allies. Over the years, we have built a strong reputation for producing action-oriented analyses and holding convenings to strengthen cybersecurity of U.S. critical infrastructure. My government career before CSIS spans leadership positions in the Pentagon's defense industrial base policy and space policy offices, the White House Office of the National Cyber Director, and the Department of Energy's National Nuclear Security Administration.

I commend New York for convening this hearing and its leading role in developing concrete regulations to protect critical water systems operated by state and local entities across the state.

Recent Water Sector Attacks Demonstrate Vulnerabilities

The topic of today's hearing is water sector security and preparedness. It goes without saying in this setting that the United States has long been vulnerable to cyberattacks on its digital networks and physical critical infrastructure. Nation-state threat actors, including Iran and China, are intent on targeting U.S. infrastructure like water and wastewater facilities due to its importance to every aspect of American life.

Water and wastewater utilities – of which there are more than 148,000 across the United States – are essential critical infrastructure that is essential to every aspect of our lives and economy.ⁱ Most Americans take for granted that other sectors like healthcare, energy, schools, emergency response, and the industrial base more broadly, rely on water for daily operations. Any disruptions to drinking water and wastewater facilities, whether caused by cyber or other incidents, can have outsized impacts that ripple across the United States.



In late July 2026, Minnesota officials were the first to report anomaliesⁱⁱ at water utilities state-wide – eventually totaling over 30 observed incidents. Over several days, federal agencies and state officials reported known cyberattacks in “at least seven” states.ⁱⁱⁱ News reports eventually placed the number at 12 states and 100 municipal water facilities affected.^{iv} The attacks were broad and relatively unsophisticated, targeting a vulnerable, internet-connected node (the programmable logic controller, or PLC) allowing utilities across America to remotely control system operations that were weakly-protected using default (or no) passwords.

While the Intelligence Community has not yet formally attributed the attacks, the CyberAv3ngers hacking group claimed responsibility for the massive campaign, writing in late July that the attacks were “only a small fraction of our capabilities” and intended as a warning amid the ongoing Middle East conflict.^v Further, Iran has demonstrated a specific interest in targeting U.S. water systems, and the Cybersecurity and Infrastructure Security Agency (CISA) updated previous warnings to water utilities just days before the attacks, urgently alerting them of Iran-affiliated groups’ intent to target PLCs.^{vi} The targeted water utilities were generally able to take their systems offline (reverting to manual operations in some cases) and maintain safe drinking water free of contamination, but the attacks were alarming for their ability to sow disruption across the United States.

This spate of attacks is noteworthy for its scale, its relatively unsophisticated tactics designed to exploit lax cybersecurity procedures, and its precedented nature. By targeting a vulnerable component widely used by American water utilities, the attackers’ intent was likely to sow confusion across states, rather than procure a targeted goal such as a ransom or financial gain. The attackers’ relatively unsophisticated tactics simply included compromising remote control capabilities and exploiting users’ weak or non-existent passwords. The attacks were also not unprecedented. In 2013, an Iranian-affiliated hacker group was indicted for compromising and accessing the control system of a dam in Rye, New York and, in 2023, CyberAv3ngers previously targeted PLCs during an attack on a Pennsylvania water system – demonstrating a clear pattern of intent and capability.^{vii}

Since the United States first launched kinetic attacks against Iran in February 2026, government officials and experts warned the regime would likely leverage its cyber capabilities – and network of aligned ‘hacktivist’ groups – to cause outsized disruption relative to its kinetic capabilities, where the United States has a significant advantage.^{viii} In addition to the water sector hacks, Iran-linked groups have claimed responsibility for targeting medical technology firm Stryker and conducting a ‘hack and leak’ operation against FBI Director Kash Patel.^{ix}



Across the United States, water utilities in the cross-hairs of cyber threat actors face many entrenched, systemic challenges. Many are operated by private entities or small local utilities that lack the resources and personnel to prioritize cybersecurity and defensive best-practices, not least when their adversaries are often sophisticated, highly-capable nation-state threat actors. This reality sits in stark contrast to the importance of these facilities in the United States and globally. The attacks also came as federal cybersecurity-focused agencies, including CISA, have been operating in a strained staffing and budgetary environment^x since before the conflict in Iran began.

Broader Cyber Threat to Critical Infrastructure

These attacks should be considered in the context of a broader cyber threat landscape, with multiple actors and different strategic objectives. Iran has a demonstrated track record targeting U.S. water systems. And, the People's Republic of China (PRC) is the most sophisticated and well-resourced threat actor the United States faces in cyberspace.^{xi} Over the past several years, U.S. Government officials have been tracking a PRC-linked group known as *Volt Typhoon* that gained access to and prepositioned themselves on critical infrastructure networks including water, energy, and communications for years, likely in order to disrupt these systems in a future conflict scenario with the United States.^{xii} Many experts believe these actors may not have been fully uprooted from U.S. networks, demonstrating their intent to maintain persistent access, rather than conduct opportunistic attacks or extract a ransom.^{xiii}

AI is also making it increasingly possible for all would-be cyber actors to enhance the speed, scope, and scale of their attacks. Since spring of 2026, revelations surrounding Anthropic's Mythos model, OpenAI's pre-release model accessing the internet and hacking its way into Hugging Face (and many other companies') networks, and the prevalence of Chinese open-weight models, have irreversibly changed the cyber threat landscape and increased the likelihood of even more frequent attacks by state and criminal cyber actors.^{xiv}

Strengthening Water Sector Cyber Resilience

Given these developments, critical infrastructure operators – including water and wastewater utilities Americans are dependent upon – must urgently prioritize cybersecurity and resilience to withstand the types of attacks described above.

In this regard, New York State is a trailblazer for setting nation-wide standards for water and wastewater sector cybersecurity and pairing them with needed resources, even as broader efforts at the national level have so far stalled. Governor Hochul's March 2026 announcement that the state would implement the first-ever water cybersecurity regulations, backed by a \$2.5 million grant to support under-resourced utilities across the state (as part of a "sector-by-sector" approach) is a powerful start. The regulation, which implements new mandatory requirements for



cyber training, incident reporting, risk-based standards to protect systems, and notably a specified cyber point of contact at large utilities, is backed by financial resources utilities need to effectively carry them out.^{xv} Then, in August, when 12 states and more than 100 facilities across the nation experienced cyberattacks, New York stepped up its own investment to inject \$9 million in additional funds to 153 utilities state-wide, demonstrating action-oriented leadership that other states would do well to follow.^{xvi} New York's standard-setting actions follow a historic lack of national leadership in setting sector-specific cybersecurity requirements.

Yet, at the same time, federal-level efforts have trailed proactive state initiatives. To date, cyber guidelines at the national level tend to be fragmented, voluntary in nature, and lacking funds to execute. The executive branch and Congress have been slow to establish national cybersecurity requirements and, crucially, pair them with needed resources (rather than provide unfunded mandates). However, following the summer water sector attacks, both Congress and the executive appear to be taking greater notice of these sector vulnerabilities, and seeking ways to empower the Environmental Protection Agency (the responsible agency for water resilience) with needed authorities. In August, Senators Adam Schiff (D-CA) and Amy Klobuchar (D-MN) introduced the 'Water Cyber Shield Act,' which would update the Safe Drinking Water Act to include cyber requirements for water and wastewater facilities.^{xvii} In 2025, Representative Rick Crawford (R-AR) spearheaded a bill to create a new Water Risk and Resilience Organization (WRRO) to set national resilience standards for the sector, and the proposal is now receiving renewed attention.^{xviii} Both efforts follow an unsuccessful 2023 attempt by the Biden Administration's EPA to mandate cyber standards for the water sector, which received immediate pushback from a coalition of governors and industry associations.^{xix} In late August, the White House Office of the National Cyber Director Sean Cairncross and Texas Governor Greg Abbot announced Project Watershed 250, which is designed to ensure Texas water operators have free access to cybersecurity resources state-wide.^{xx} While such actions are promising, they will need to be sustained beyond the current moment – and paired with scalable and sustainable national solutions to meet the severe challenges water utility operators across the country face.

Conclusion and Recommendations for State and Federal Policymakers

The attacks the United States experienced this summer - in the context of an ongoing kinetic conflict in the Middle East - should be both a wake-up call and an opportunity. Rather than consider cybersecurity of critical water utilities a "tomorrow" problem, critical infrastructure owners and operators should assume they are targets today and act accordingly.

Going forward, New York should continue down the proactive path to which it is already committed by developing clear, risk-informed requirements for local operators and pairing them with the resources needed to operationalize them.



In the short-term, water and wastewater utility operators in New York and nation-wide should implement basic cybersecurity hygiene even as state- and nation-wide initiatives take shape: specifically, local utilities should disconnect their internet-facing PLCs (or other remotely controlled technology) whenever possible; they should ensure systems are protected with passwords that are strong and unique across systems; critical water and wastewater systems should be actively monitored; and, operators should monitor their systems for anomalous activities and report them to state- and federal-level authorities including the FBI, CISA and the EPA. Perhaps most importantly, the executive branch and Congress should act urgently to empower federal agencies like the EPA and establish minimum cybersecurity standards for the water sector nationwide, pairing these with appropriate funding and technical resources nationwide (for example, expanding Project Watershed 250 beyond Texas).

Over the medium and long-term, federal agencies should partner more closely with state and local entities to ensure they receive the appropriate threat intelligence to protect against nation-level threat actors. And, they should also work to strengthen the cyber workforce talent pipeline, including by investing in K-12 educational programs. With critical infrastructure already vulnerable, and nation-state actors demonstrating consistent intent and capability to target the water sector, the nation cannot afford to wait.

Thank you for the opportunity to provide my testimony and I look forward to answering your questions.

Lauryn Williams

Deputy Director & Senior Fellow, Strategic Technologies Program
Center for Strategic and International Studies (CSIS), Washington, D.C.

ⁱ [Information about Public Water Systems | US EPA](#)

ⁱⁱ https://www.minnpost.com/drinking-water/2026/07/cyberattacks-on-minnesota-water-systems-investigated-as-officials-warn-about-iranian-hackers/?gad_source=1&gad_campaignid=9109082086&gbraid=0AAAAADo2Co-qNOSu2S80rKiyEw65_UV_k&gclid=CjwKCAjww-3VBhAcEiwAwUUIu06bQDjrrJdZwLh5dxNkJnBgoXDWOvkl2hm7HN10SWDb0FXsFqUb2RoCdZUQAvD_BwE

ⁱⁱⁱ <https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet-facing-programmable-logic-controllers-causing-operational-disruptions>

^{iv} <https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet-facing-programmable-logic-controllers-causing-operational-disruptions>;
<https://www.csis.org/analysis/mapping-iranian-cyberattacks-us-water-systems>



- v <https://threatbeat.com/attacks-and-incidents/minnesota-water-attacks-were-only-to-warn-iran-hackers-claim-while-taking-responsibility/>; <https://threatbeat.com/attacks-and-incidents/minnesota-water-attacks-were-only-to-warn-iran-hackers-claim-while-taking-responsibility/>
- vi <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a>
- vii <https://www.cbsnews.com/news/iranian-cyberattacks-timeline-u-s-companies-water-systems-minnesota-hacked/>
- viii <https://www.lawfaremedia.org/article/digital-domains-are-the-new-battlefield>
- ix <https://www.cnn.com/video/2026/03/12/weighing-irans-cyber-warfare-threat-after-stryker-attack.html>; <https://www.bing.com/ck/a?!&p=f838b156ce44a029f51e09ee610e9b3cd8dea2cc3eb229c1609cfe401eb7bf0eJmltdHM9MTc5MDcyNjQwMA&ptn=3&ver=2&hsh=4&fclid=1b92dc02-6242-65cb-1bd9-cb7b630364b6&psq=kash+patel+hack+and+leak&u=a1aHR0cHM6Ly93d3cuYmJlLmNvbS9uZXdzL2FydGljbGVzL2N2Z2w0eWs3dmdwbw>
- x <https://www.washingtonpost.com/opinions/2025/11/20/shutdown-cyberattacks-china-trump-administration-cuts/>
- xi <https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>
- xii <https://www.csis.org/analysis/iran-conflict-heightens-cyber-threats-us-energy-infrastructure>
- xiii [Researchers warn Volt Typhoon still embedded in US utilities and some breaches may never be found | The Record from Recorded Future News](#)
- xiv <https://www.csis.org/analysis/chinas-open-weight-challenge-us-ai-leadership>
- xv <https://www.governor.ny.gov/news/governor-hochul-announces-first-nation-cybersecurity-regulations-and-grants-protect-new-york>
- xvi <https://www.youtube.com/watch?v=3UJ6Uc2FBe0>
- xvii <https://www.congress.gov/bill/119th-congress/senate-bill/5368/text>
- xviii <https://www.congress.gov/bill/119th-congress/house-bill/2594/text>
- xix <https://cyberscoop.com/epa-water-cyber-regulations/>
- xx <https://gov.texas.gov/news/post/governor-abbott-national-cyber-director-launch-project-watershed-250-to-defend-texas-water-supply>