

CYBERSECURITY

Internal deliberative pre-decisional - FOR USE BY 2024 PRESIDENT-ELECT TRANSITION TEAM MEMBERS ONLY

ISSUE SUMMARY:

The water sector is at high risk from cyber-attacks: attacks sponsored by, affiliated with, or supportive of adversarial nation states have disrupted US water and wastewater services. EPA by statute and Presidential Order has the lead federal responsibility for protecting the water sector from cyberattacks, with the bulk of this responsibility residing in the Office of Water.

KEY POINTS:

- Cyber-attacks represent a high risk for the sector because water and wastewater facilities use automated process controls and electronic networks to monitor and operate virtually all aspects of their operating systems, and most of the water sector has failed to adopt basic cybersecurity practices despite over a decade of extensive technical assistance from EPA and DHS.
- Groups associated with China, Russia, and Iran are actively seeking access to US critical infrastructure including specifically water and wastewater systems, with China designated by US Intelligence as the most advanced and persistent threat: China is understood to wish to disrupt US water sector services in the event of a geopolitical conflict.
- As evident from both an industry survey conducted in 2021 and from actual cyber incidents, many water and wastewater systems have failed to adopt even very basic cybersecurity practices.
 - A survey administered by the Water Sector Coordinating Council—the primary stakeholder forum for water security—found that just 22% of respondents had fully implement a cybersecurity program, while only 30% of respondents had inventoried their internet facing operational technology (OT) networks.
 - In 2023, CyberAv3ngers, a cyberterrorist organization affiliated with the Iranian Revolutionary Guard Corps, managed to access nearly 20 water and wastewater systems—including disabling a small rural water system in Illinois—by exploiting the fact that these systems neglected to change a publicly known password of 1111 in a programmable logic controller (PLC).
 - In 2024, the pro-Russia hacktivist group, the Cyber Army of Russia Reborn, gained access to several water and wastewater systems and succeeded in manipulating the systems' industrial controls, for example, causing a water tank to overflow at a small water system in Texas and a lift station to malfunction at a small wastewater system in Indiana.
- Under the federal national security structure, each of the 16 critical infrastructure sectors (energy, healthcare, communications, etc) has a Sector Risk Management Agency (SRMA) which serves as the federal lead agency responsible for enhancing that sector's security and resilience to physical and cyber threats: EPA is the SRMA for the water sector which includes about 150,000 water systems and 16,000 wastewater systems, and the Water Infrastructure and Cyber Resilience Division in the Office of Water (OW) serves as the Agency's primary lead for fulfilling this national security mission.
- OW provides an array of cyber tools, guidance, training, and direct technical assistance to assist water and wastewater systems, including:
 - OW conducts cybersecurity assessments at utilities through the *Cybersecurity Evaluation Program* where utilities work with an EPA cybersecurity professional to conduct cybersecurity assessments and prepare a Risk Mitigation Plan so the utilities can systematically address their cybersecurity gaps.

- To date, EPA has conducted over 300 cybersecurity assessments at water and wastewater systems: several states, e.g., West Virginia, Oklahoma, and Massachusetts, have requested that EPA provide assessments of their water systems.
- OW has the primary federal responsibility for developing cybersecurity alerts for the water sector: for instance, OW co-authored (with DHS, FBI and NSA) and distributed an alert to upwards of 60,000 water and wastewater systems and the states on the Volt Typhoon cyberattacks associated with China, and conducted a webinar (with over 1,000 attendees) to underscore the severity of the threat and the mitigation measures available to reduce the risk of a cyberattack.
- OW coordinates with the Department of Defence on developing a cybersecurity technical assistance initiative targeted to water and wastewater systems serving about 110 defense critical infrastructure (DCI) facilities across the US states and the territories, and partners with the US Coast Guard in delivering cybersecurity assistance to Guam to protect the water infrastructure supporting the Navy and Air Force bases on the island.
- OW developed the easy-to-use *Water Cybersecurity Assessment Tool* (WCAT) at the request of the water sector to enable water systems to self-assess their cybersecurity practices: states and technical assistance providers also use this tool when conducting cybersecurity assessments at water systems.
- OW also offers direct technical assistance through the *Cybersecurity Technical Assistance Program* for the Water Sector: states, technical assistance providers, and utilities may submit cybersecurity questions and then receive one-on-one, immediate assistance from an EPA cybersecurity subject-matter expert.
- OW provides cybersecurity exercises which cover threat actor intent and capabilities, common vulnerabilities exploited by state and non-state actors, how to conduct cybersecurity assessments, and the most effective cybersecurity countermeasures: to date, EPA has provided these exercises to over 3,000 water and wastewater utilities.
- OW coordinates closely with the DHS Cybersecurity and Infrastructure Security Agency (CISA) and FBI in responding to cyberattacks against water and wastewater systems: for instance, in response to the SolarWinds cyberattack, EPA contacted the over 70 water sector entities affected to confirm that they were aware of the attacks and had undertaken the necessary mitigation measures.
- OW reviews classified threat intelligence information on a frequent basis to ensure that EPA provides exercises, tools, and technical assistance which effectively address the types of threat actors and common vulnerabilities exploited by these actors.
- OW provides training for technical assistance providers (e.g., National Rural Water Association circuit riders) on how to conduct cybersecurity assessments at small, rural water and wastewater systems.
- EPA's enforcement office, in coordination with OW, issued in 2024 an enforcement alert to announce increased inspections of water systems' cybersecurity practices: OW has provided technical expertise, including training of EPA inspectors, in support of this initiative.
- EPA's Office of National Security (ONS) and OW engage directly with the White House National Security Council and the Intelligence Community (IC) to identify and share information and intelligence, classified and unclassified, with EPA programs and regions, water sector partners and other federal agencies. ONS leads EPA's Intelligence Coordinating Network (ICN), comprised of subject matter experts and intelligence consumers from program offices and regions to enhance the internal/external exchange of intelligence information at EPA. The ICN supports intelligence sharing related to the water and wastewater sector. ONS manages the Cyber Threat Intelligence (CTI) Program which provides comprehensive insights into cyber threats targeting federal agencies and the water sector. CTI supports the Office of Water's efforts to enhance the security posture of the Nation's water and wastewater sector's (WWS) critical infrastructure.

ONGOING/UPCOMING REVIEWS FOR FY2024:

EPA has formed a Cybersecurity Task Force between the private and public sectors to prioritize near term actions, identify collaborative opportunities among federal/state/local/private/association representatives, and find gaps in current activities and means to close such gaps: the final report will be available by October 2024.

KEY EXTERNAL STAKEHOLDERS:

- | | | | | | |
|----------------------------------------------|-------------------------------------------------------|--------------------------------------------|--------------------------------------------|-------------------------------------------|----------------------------------------------------------|
| <input checked="" type="checkbox"/> Congress | <input checked="" type="checkbox"/> Industry | <input checked="" type="checkbox"/> States | <input checked="" type="checkbox"/> Tribes | <input checked="" type="checkbox"/> Media | <input checked="" type="checkbox"/> Other Federal Agency |
| <input type="checkbox"/> NGO | <input checked="" type="checkbox"/> Local Governments | <input checked="" type="checkbox"/> Public | | | |

MOVING FORWARD:

EPA will offer direct technical assistance to water and wastewater systems through its Cybersecurity Evaluation Program and Cybersecurity Technical Assistance Program services, will conduct training of enforcement inspectors to identify and mitigate the risks of cyber-attacks, will implement action items from the Cybersecurity Task Force, and will continue to provide technical assistance to Congress regarding EPA's cybersecurity authorities.