Q1 2025

# Water & Wastewater Sector

*A Quarterly National Security Information-Sharing Bulletin from the U.S. Environmental Protection Agency and the Water Information Sharing and Analysis Center*

## In This Issue



## We All Play a Role in Supporting National Security and Resilience

As threats to critical infrastructure continue to rise and with cyber actors showing an increased interest in operational technology (OT) and industrial control systems (ICS), it is now more important than ever for all of us to develop a security mindset and do our part to protect the nation's critical infrastructure. We all play a role in supporting national security, whether we realize it or not. In the government, we are seeing efforts to increase vetting and oversight of activities of third-party vendors and managed service providers. Countless stakeholders have emphasized that the water and wastewater sector needs more resources in order to provide security training, obtain technical assistance, and to secure support from outside vendors to assist with cybersecurity for information technology (IT) and OT systems.

The water and wastewater sector is a lifeline for the functioning of society and due to the vulnerabilities inherent to the sector, it has become a target for cyber actors who want to make money from ransomware attacks or to gain leverage ideologically or geopolitically. In an effort to improve efficiencies, the sector often leverages third party vendors to support their IT and OT operations. Consequently, an often overlooked area in the sector's cybersecurity posture is the potential for these third party vendors or integrators to create vulnerabilities when they utilize remote access to perform activities such as system monitoring and routine maintenance. Vendors may not be as mindful of the utility's security protocols and may leave a utility's IT or OT devices exposed to the internet. A cyber actor could exploit this insecure remote access and cause operational impacts such as a disruption of service or encrypt access to these devices for a ransom. Owners and operators as well as utility and municipal leadership all need to ensure their contracts with third-party vendors include robust cybersecurity protocols in line with their utility's.

In addition to cyber threats, a wide range of physical threat actors are also targeting the sector, with motivations ranging from ideological objectives, political beliefs, personal grievances, or financial incentives. Utilities must continue to have a strong posture to prevent or mitigate physical impacts from external actors and insider threats. The threats are complex because the threat actors know the negative impacts a successful attack will have on society.

Reporting incidents is critical to preventing future attacks. It also helps others in the sector be more prepared to respond and recover in the event of a similar threat. Maintaining the public's trust in critical infrastructure and protecting our nation's water supply and our wastewater treatment systems is a responsibility we all share. Protecting the public and expanding our approach to security whether by combatting physical, cyber, or insider threats is critical to support the nation's national security and resilience.

# CISA and EPA Release Joint Fact Sheet Detailing Risks Internet-Exposed HMIs Pose to Water and Wastewater Sector

In December, 2024, CISA and the EPA released a joint fact sheet titled "Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems." The fact sheet offers guidance to water and wastewater utilities on how to minimize the exposure of human-machine interfaces and protect them from cyber threats. As various threat groups and hacktivists have **targeted the water and wastewater (WWS) sector**, WaterISAC and EPA strongly encourage utilities to review the fact sheet and its guidance.

To understand the extent of exposed ICS devices, take a look at this **Censys data** WaterISAC recently shared: "the **2024 State of the Internet Report** from Censys reveals data of over 145,000 internet-exposed ICS devices globally, with more than one-third located in the U.S. alone." While this data is troubling, the real number of exposed ICS is known to be much higher, as shown by the **PLCHound** researchers.

To mitigate the risks of cyber attacks, water and wastewater utilities are advised to inventory all internet-exposed devices, disconnect HMIs and other unprotected systems from the internet or secure them with strong usernames and passwords, and use multi-factor authentication (MFA) for HMIs and for the entire OT network.

Water and wastewater utilities are encouraged to review the fact sheet and implement the actions listed in the mitigations section. ***Access the full fact sheet at CISA.***

# Salt Typhoon: The Escalating Chinese Cyber Threat to U.S. National Security and Critical Infrastructure

The Salt Typhoon cyber-attack campaign, attributed to Chinese state-sponsored cyber actors, poses a severe and escalating threat to U.S. national security. The breach has expanded to affect at least nine major U.S. telecom companies as of January 2025, compromising sensitive communications of high-profile government and political figures. The attackers gained access to extensive customer metadata, potentially exposing U.S. government surveillance targets and jeopardizing ongoing law enforcement investigations.

This widespread infiltration extends beyond telecommunications, raising concerns about the vulnerability of other critical infrastructure sectors. U.S. officials warn that these intrusions could be preparation for future disruptive cyber attacks, possibly aimed at hindering U.S. military mobilization during a conflict.

The ongoing Salt Typhoon threat serves as a stark reminder of the critical importance of proactive cybersecurity measures in safeguarding national security interests. Key recommendations to counter this threat include implementing robust network segmentation, ensuring regular patching of all systems, enforcing multi-factor authentication, enhancing logging and monitoring capabilities, and adopting encrypted communication tools for sensitive information exchange. These measures are designed to create a more resilient infrastructure capable of withstanding and detecting sophisticated cyber intrusions. The

persistent nature of this threat underscores the need for continuous adaptation and improvement in defensive strategies to counter the evolving dangers posed by state-sponsored cyber actors, emphasizing that cybersecurity must be an ongoing, dynamic process to effectively protect critical infrastructure.

*For more information, consult the CISA guidance document and explore additional details about cyber actors associated with the People's Republic of China.*

Additional Reading:

- **More telecom firms were breached by Chinese hackers than previously reported**
- **Salt Typhoon Chinese Cyber Espionage Team Named in T-Mobile Hack; Group Breached All Three Major US Carriers**

# The Rising Physical Security Threat to Critical Infrastructure from Drones

Drones, or unmanned aircraft systems (UAS), are now ubiquitous around the world and used for a variety of legitimate purposes. However, as prices decrease and more drone models become available, both state and non-state actors are increasingly utilizing these systems to conduct malicious activities, including the targeting of critical infrastructure.

Underscoring this increasing threat, in November, a suspected domestic violent extremist (DVE) was arrested and charged in federal court for attempting to destroy an electric substation in Nashville by using an explosive-laden drone he built himself. Consequently, explosive-laden drones represent one of the most lethal aspects of the drone threat. Indeed, many of the drones used in the conflicts in Ukraine and the Middle East often come in the form of small, commercially available, remote-controlled aircraft. They're either outfitted with a small explosive to be dropped onto a target or are simply crashed into it as a self-detonating, one-way attack drone.

In addition to using drones for explosive attacks, terrorists and other threat actors can attach sensors for intelligence, surveillance, and reconnaissance (ISR) purposes; or hook up a camera or speaker for propaganda activity. For example, a suspected DVE who pleaded guilty in federal court for firebombing a Planned Parenthood clinic, reportedly used a drone to conduct reconnaissance of an electric substation he

was also planning to attack. Moreover, drones made in China could pose a cybersecurity and physical security risk to critical infrastructure operators in the West.

Although there are currently few counter drone solutions available to the private sector, many products are in development. Some of these solutions range from communication-jamming equipment to guns that shoot rapidly expanding nets to experimental lasers. Still, under current law, that authority is generally limited to federal agents. In the event of an incident, organizations are strongly encouraged to contact local law enforcement to address immediate security and safety concerns. ***To help manage drone-related security risks read more at CISA or read a related article at Domestic Preparedness***.

## Insider Threat Corner

Many water and wastewater utilities receive services from third-party vendors. The services they provide may range from cleaners and auditors to cyber security services. While these vendors are being paid and are under contract, it's still imperative to provide oversight to ensure they are doing what they are tasked. These vendors can serve as witting or unwitting threats to the utility. It is imperative to fully understand the terms and conditions of their services so you know the limits and requirements of the contract. In addition, do not assume a vendor has security baked in their terms. Vulnerabilities presented by third parties range from unlocked access points, open network ports, access to confidential business information, or even access to switches and valves.

The following are some things to consider when using third-party vendors:

- Utilities should foster a culture of security and best practices.
- Oversight of services must be conducted constantly and continuously.
- Thorough vetting must be conducted prior to accepting the contract to ensure trustworthiness.
- A comprehensive review must occur to ensure the services provided are what is needed and are appropriate.
- See something say something.

***Read more about Insider Threats at CISA here***.

# National Counterintelligence Strategy

The National Counterintelligence and Security Center (NCSC) released a National Counterintelligence Strategy, describing the approach used by the intelligence community (IC) to protect America's strategic advantages. Historically, counterintelligence was seen as the FBI or the intelligence community searching for spies. Today, it is clear that the complex nature of the threats facing the U.S. has caused the counterintelligence community to expand efforts to integrate and collaborate across areas such as cybersecurity, emerging technology, critical infrastructure protection, and supply chain risk management, among others.

The U.S. counterintelligence community is charged with identifying, understanding, and neutralizing foreign intelligence activities and capabilities in the U. S.; mitigating insider threats; protecting U.S. sensitive and classified information and sensitive facilities from technical penetrations, espionage, and other intelligence threats; and protecting U.S. interests, assets, and people at home and abroad from sabotage, assassination, or other foreign intelligence activities or operations. Now counterintelligence activities require engagement by a broader set of stakeholders and the counterintelligence community must engage partners and audiences across the whole of society to share information, identify and mitigate vulnerabilities, strengthen our defenses and build resilience, and work together to combat these threats and overcome challenges to protect our people, institutions, and strategic advantages.

**Goal 7 of the strategy, "Protecting the Nation's Critical Infrastructure", describes protection of critical infrastructure including water and wastewater systems, against potential attacks by foreign intelligence entities**. The area of defense has broadened as adversaries target an expanding range of public and private sector entities and employ numerous avenues of approach, all while we are using more connected devices and remote platforms that put our data, networks, and infrastructure at risk.

Foreign intelligence entities (FIEs) seek to collect information from virtually all public and private entities involved with critical infrastructure. Adversaries target classified information and unclassified material to support their goals and attempts to target U.S. persons, supply chains, and critical infrastructure.

Adversaries use advanced technology, including cyber tools, biometric devices, unmanned systems, high-resolution imagery, enhanced technical surveillance equipment, commercial spyware, and

Artificial Intelligence (AI) to further their espionage, counterespionage, and influence missions.

Insider threats pose a significant vulnerability. In some cases, insiders use their authorized access, wittingly or unwittingly, to do harm to the security of the U. S. In other cases, FIEs actively target, solicit, and coerce individuals to obtain information, compromise critical infrastructure, or steal secrets. For example, in November, a Florida man was sentenced in federal court for conspiring to act as an agent of the People's Republic of China (PRC) for over the past decade. The individual worked at a telecommunications firm, among other places, and notably shared materials relating to cybersecurity training at his company with Chinese intelligence operatives. Insider threats can also be third-party vendors or managed service providers.

This strategy states that as the threat to critical infrastructure grows, the IC is encouraged to develop and maintain robust partnerships across the public and private sector to better understand critical infrastructure sectors and how foreign intelligence entities may target them. This new expanded partnership approach is intended to improve information sharing and data integration to gain deeper insight into interdependencies between sectors and vulnerabilities and threats from foreign intelligence entities to critical infrastructure. ***Read the full National Counterintelligence Strategy here***.

# CISA Requests Public Comment for Draft National Cyber Incident Response Plan Update

CISA—through the Joint Cyber Defense Collaborative and in coordination with the Office of the National Cyber Director (ONCD)—released the **National Cyber Incident Response Plan Update Public Comment Draft**. The draft requests public comment on the National Cyber Incident Response Plan (NCIRP), which is open now for public comment and concludes on February 14, 2025.

Since initial publication in 2016, CISA conducted broad and extensive engagement and information exchanges with public and private sector partners, interagency partners, federal Sector Risk Management Agencies (SRMAs), and regulators to build upon the successes of the inaugural NCIRP. The draft NCIRP update describes a national approach to coordinating significant cyber incident detection and response.

The draft update considers the evolution in the cyber threat landscape and lessons learned from historical incidents. The text also addresses the vital role that the private sector, state and local governments (including tribal and territorial), and federal agencies hold in responding to cyber incidents.

CISA is seeking more perspectives to help strengthen the NCIRP and invites stakeholders from across the public and private sectors to share their knowledge and experiences, further informing our findings and contributing to this revision. ***Public comments may be posted via the Federal Register***.

# Response and Recovery from Natural Disasters

In 2024 (as of November 1), there were 24 confirmed weather/climate disaster events with losses exceeding $1 billion each to affect United States. In October of 2024, Hurricane Helene alone caused 256 counties across 6 states to be declared major disaster areas. Water and wastewater utilities throughout this region were **significantly impacted** by this storm.

Thankfully, Water and Wastewater Agency Response Networks (WARNs) across the impacted areas sprang into action and responded to the disaster to help local communities and utilities recover. **WARNs are statewide utility-to-utility** mutual aid and assistance networks. A mutual aid and assistance network provides water and wastewater utilities with the means to quickly obtain help during an emergency. If you are not already part of your state's WARN, it is highly encouraged you become a member of your WARN. There is no cost to join.

As communities recover from these disasters, Federal assistance is coordinated through the National Disaster Recovery Framework (NDRF). After disasters, impacted communities and states may be overwhelmed and may find it challenging to access the many Federal programs available to assist recovery. For this reason, Federal agencies coordinate under the NDRF to streamline Federal assistance and see how Federal programs can work together to assist recovery. For example, EPA and FEMA renewed a Memorandum of Understanding

(MOU) on September 11, 2024, that streamlines coordination between FEMA and the EPA-funded State Revolving Fund (SRF) programs so that funding to restore vital water infrastructure can be provided as quickly as possible after times of disaster.

Lastly, to help utilities identify the most appropriate federal funding for recovery or hazard mitigation efforts, EPA maintains a "Federal Funding for Water and Wastewater Utilities in National Disasters," webpage that presents information tailored to water and wastewater utilities on federal disaster and mitigation funding programs from EPA, FEMA, HUD and SBA. ***Access the EPA funding page here***.

# Useful Links and Contact Information

For feedback, comments or questions related to the content in this bulletin, please email Water-NSISB@epa.gov

## WaterISAC

Website | www.waterisac.org/

Membership Information | www.waterisac.org/membership

Incident Reporting Form | www.waterisac.org/report-incident

24 Hour Line | 866-H2O-ISAC

### EPA

Office of National Security | www.epa.gov/national-security

Drinking Water and Wastewater Resilience Website | www.epa.gov/waterresilience

Cybersecurity for the Water Sector | www.epa.gov/waterresilience/epa-cybersecurity-water-sector

## Water Sector Coordinating Council

- American Water Works Association
- Association of Metropolitan Water Agencies
- National Association of Clean Water Agencies
- National Association of Water Companies
- National Rural Water Association
- Water Environment Federation
- WaterISAC
- Water Research Foundation