September 2024

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

Why Are We Sending Out an Information Sharing Bulletin on National Security?

The purpose of this Information Sharing Bulletin (ISB) is to support the goals and objectives of National Security Memorandum (NSM)-22-Critical Infrastructure Resilience. Namely, that the federal government will support a robust information sharing environment and public-private cooperation. "Information sharing" does not simply mean the timely sharing of intelligence and threat information, but also sharing developments in national resilience efforts, national security policies, open-source intelligence and threat assessments (or publicly available threat reporting of relevance). Furthermore, it includes updates regarding geopolitical events that may ultimately have an impact on water and wastewater infrastructure.

The ISB is intended for water and wastewater utility operators to provide them with information on priority security and resilience topics, including cybersecurity, physical security, and natural disasters. It is designed to increase awareness of these priorities and promote a security mindset across all utility staff and the water and wastewater sector to better prepare for and respond to ever-increasing threats. Utility leaders and staff with responsibilities in any of these areas can use the ISB to obtain additional context on the foremost issues involving the sector. However, all utility staff can benefit from reading its contents and learning about the latest developments, especially since security and resilience should be a team effort. Therefore, the authoring organizations encourage utilities to disseminate this ISB as widely as possible among staff and to partners.

The EPA Office of National Security (ONS), the EPA Office of Water, WaterISAC, and the Water Sector Coordinating Council and Government Coordinating Council (WSCC) have initiated this effort to raise awareness on existing and emerging issues. Their goal is to inform and drive efforts to enhance preparedness and resilience within the water and wastewater sector and across the 16 domestic critical infrastructure sectors in the U.S. For more information on what the various organizations supporting the ISB do, please see the links at the bottom of the page.

The Great Lakes seen from space. Photo credit: NOAA

Stat of the Quarter

Implement a cybersecurity framework to reduce your cyber vulnerability. CLICK HERE

Cyberattacks on Water Sector Rise in 2024

In recent months, the United States has seen a concerning rise in cyberattacks targeting water and wastewater systems across the country. The Environmental Protection Agency (EPA) warned earlier this year the sector is facing an increasing number of cyber attacks and incidents. These attacks have ranged from ransomware incidents to unauthorized access attempts, with some disrupting water services.

One notable incident occurred in a small Pennsylvania town in late 2023, where an Iranian-linked group called "Cyber Av3ngers" targeted a local water provider. This attack forced the utility to switch from automatic pump operations to manual control, highlighting the potential for disruption in critical infrastructure.

More recently, a Russian-linked hacktivist group, Cyber Army of Russia Reborn compromised operations at several utilities across the country, further demonstrating the geopolitical dimensions of these cyber threats.

The tactics employed by attackers have varied. Some have exploited vulnerabilities to gain unauthorized access to control systems, as seen in the Pennsylvania incident. Others have used ransomware to disrupt operations and extort money from water utilities. In some cases, attackers have attempted to alter chemical levels in water treatment processes, posing potential public health risks.

As the threat landscape evolves, protecting critical infrastructure and public health remains paramount. Collaboration between federal, state, and local entities, along with increased resources and training, will be crucial in building resilience against cyber threats in the water sector.

Diverse Set of Terrorist and Violent Extremist Threat Actors Driving Heightened Threat Environment

A diverse set of terrorist and violent extremist threat actors increasingly seek to inspire and conduct attacks or other malicious activity against the U.S. and its Western partners in furtherance of their ideological goals. This widening range of threat actors, including domestic violent extremists (DVEs), homegrown violent extremists (HVEs), and foreign terrorist organizations (FTOs) motivated by various socio-political dynamics, are driving the heightened risk of extremist targeted violence.

Several socio-political dynamics are galvanizing terrorists and violent extremists to action from across the ideological spectrum. Some of these socio-political dynamics include the ongoing Israel-Hamas conflict, the upcoming U.S. political elections, among other causes. These events coupled with the broadening reach of violent extremist online propaganda is very likely to drive HVE and DVE threat actors into conducting physical threat activities throughout 2024, according to a report from the cybersecurity firm Recorded Future.

In addition, in March, four Islamic State gunmen conducted a terrorist attack in Russia that left hundreds dead. Given these developments, FBI Director Christopher Wray warned the U.S. government is increasingly concerned about the "potential for a coordinated attack here in the homeland, akin to the [Islamic State] attack we saw [in Russia]." Additionally, increasing FTO media encouraging supporters in the West to launch attacks, coupled with recently thwarted terrorist plots and arrests in the U.S. and Europe, underscores the enduring risk of extremist targeted attacks motivated by international terrorism.

DVEs also continue to present one of the most lethal threats of extremist targeted violence to the U.S. homeland. In particular, many DVEs continue to call for and plot attacks against critical infrastructure to advance their ideological agendas. Amid this heightened threat environment, facilities and personnel associated with critical infrastructure are at elevated risk from HVE and DVE physical threat activities, which should encourage owners and operators to maintain heightened vigilance.

Read more at Recorded Future, at the Global Network on Extremism and Technology, at George Washington University, at Foreign Affairs, at the Washington Institute of Near East Studies, and at CNN.

Recent Floods Put Spotlight on Impacts to Wastewater Utilities, Need for Greater Resilience

In June, torrential rain across parts of the Midwest led to extensive flooding, resulting in widespread and notable impacts to wastewater utilities. Between 10 and 18 inches of rain fell in places where soils were already saturated from months of wetter-than-average conditions, sending runoff into streams and rivers. All told, more than 150 wastewater treatment plants were impacted by these events, forced to release untreated sewage into nearby waterways.

While the attention following severe storms often focuses on the availability of other critical services, the events in June and at other times remind us of the significant impacts they can have on wastewater utilities. In the aftermath of Hurricane Maria in 2017, more than a third of wastewater treatment plants in Puerto Rico were unable to function and raw sewage flowed into waterways. In 2022, wastewater utilities across the U.S. were affected following "1-in-1,000 year" flood/rain events, such as in eastern Kentucky.

Increasingly frequent and intense storms demonstrate the need for greater investments in resilience. EPA has provided numerous helpful resources to get started, such as through its Creating Resilient Water Utilities (CRWU) initiative. EPA also published *Flood Resilience: A Basic Guide for Water and Wastewater Utilities*, which helps utilities examine the threat of flooding, determine impacts to assets, and identify cost-effective mitigation options. Although these investments can entail significant costs, they can prevent even greater expenses. The National Institute of Building Sciences recently reported natural hazard mitigation saves $4 to $11 in avoided future losses for each $1 invested. 💧

Understanding Insider Threats and Ways to Manage the Risk

In 2019, September was delegated as National Insider Threat Awareness Month (NITAM). During NITAM, federal agencies and industry work collaboratively to emphasize the importance of preparing the workforce to **deter**, **detect**, and **mitigate** threats posed from trusted insiders. The NITAM is also a reminder to emphasize the critical role employees have for insider threat defenses.

Deter: Proactive workforce engagement balanced with a strengthened security posture.

Detect: Capability to identify potential risks and concerning behaviors and recognize all forms of the threat.

Mitigate: Strategic response to manage insider risk and eliminate threats to yield a positive outcome.

An insider threat can be an individual or group who uses their authorized access, intentionally or unintentionally, to do harm to an organization. Impacts from insider threats include, but are not limited to, resource degradation, potential injury to persons or loss of life, reputational damage, and negative impacts to public health. Insider threats could manifest as current or former employees, temporary workers, volunteers, contractors, or any other individuals with privileged access.

Water and wastewater utilities have experienced impacts from insider threats, which can manifest in both the physical and cyber domains. For example, at a large combined utility, a disgruntled water utility employee was arrested on charges earlier this year after he allegedly tampered with the utility's drinking water supply. And a cyber incident from last summer involved a former water utility employee who was charged for reportedly accessing the network of the utility he used to work at and then purposefully uninstalling the main operational and monitoring system for the water treatment plant.

To help mitigate the risk of an insider threat, organizations are encouraged to establish an insider threat awareness program, which consists of two key components. First, awareness training should incorporate recognizing potential indicators of insider threats and suspicious activity behavior. Utilities can use the U.S. government's violent extremist mobilization indicator guide to help with awareness training. Second, organizations should institute clearly defined policies for employees to report suspicious behaviors to appropriate authorities. To help with that, utilities are encouraged to review CISA's free resources for creating an insider threat awareness program. 💧

Protecting Critical Infrastructure During "Multidomain" Operations

A newly published article by a U.S. military strategy expert calls for increased preparedness, including through the use of artificial intelligence (AI), against future threats to U.S. domestic critical infrastructure during international conflict situations.

The article by Mark O'Brien, a survivability analyst, is available on the website of the Homeland Defense and Security Information and Analysis Center, a Pentagon think tank. The article analyzes threats to domestic critical infrastructure within the context of what the author calls an "expanded battlefield" or "multidomain operations."

O'Brien argues the United States will soon be facing what he terms an "unstructured" international environment, in which he says lines between conflict and peace will be "blurred." He argues this environment will result in what he terms "multidomain" conflict operations that extend beyond traditional battlefield concepts. O'Brien says multidomain attacks against the United States will include use of information warfare, cyber-attacks, and the deployment of low-cost weapons, like drones, by adversaries. The author says the United States, as a result can no longer regard its geographical position between two oceans as a sanctuary from attacks in an expanded threat environment.

O'Brien argues that the CISA-defined 16 critical infrastructure sectors would constitute prime targets for U.S. adversaries during a multidomain conflict, thus requiring extensive protection efforts. He says future threats to critical infrastructure could also take the form of chemical, nuclear, or biological attacks.

In response, the author lists a series of recommendations for action. These include increased coordination among critical infrastructure partners, sufficient intelligence capabilities, and increasing the critical infrastructure resilience of military facilities. The article also recommends the use of AI technologies and their data capabilities to enhance protection efforts. 💧

Safety and Security Guidelines for Critical Infrastructure Owners and Operators

A new guide from the Cybersecurity and Infrastructure Security Agency (CISA) calls on critical infrastructure managers to create Artificial Intelligence (AI) risk management protocols as part of a larger culture of AI safety.

CISA's *Safety and Security Guidelines for Critical Infrastructure Owners and Operators* identifies three overarching categories of cross-sector AI risk: Attacks using AI; attacks targeting AI systems; and failures in AI design and implementation. The guide says operators should consider these categories when implementing AI risk management guidelines.

Specific risks include: AI-driven social engineering; the use of AI to develop weapons or other harmful materials for a physical attack; and theft of confidential or sensitive critical infrastructure data from AI systems.

The CISA guide says organizations should develop risk management guidelines and protocols based on a keen understanding of both an organization's specific AI use and of its AI risk profile. 💧

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