TLP:CLEAR

Q3 2026

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

This quarter's *National Security Information Sharing Bulletin* centers on artificial intelligence (AI) as both a growing threat and a defensive tool for the water and wastewater sector. Our feature article examines how AI is reshaping the cyber-threat landscape — lowering the barrier to entry for attackers, accelerating reconnaissance and exploitation, and improving social engineering and ransomware operations — while also exploring how utilities can harness AI for continuous threat detection, sensor analytics, and faster incident response. The issue's featured interview is with three water utility IT directors discussing threat trends, IT and operational technology (OT) convergence, incident response, workforce culture, and low-cost risk reduction for resource-constrained systems.

This issue also covers a CISA alert on active targeting of internet-exposed programmable logic controllers (PLCs), guidance on safeguarding sensitive operational data amid AI-related public records requests, the growing physical security threat posed by drones and drone swarms, and EPA and NIST resources to help utilities build AI security into their existing risk management programs. It closes with an overview of how AI is reshaping insider threat risk.

As always, WaterISAC and EPA encourage utilities to use this bulletin to inform training, planning, and board-level conversations about cybersecurity and physical security improvements.

The New Threat Landscape: AI Security in the Water and Wastewater Sector

AI is fundamentally transforming the cyber-threat landscape for all industries, including the water and wastewater sector. It is already enabling attackers to operate faster, at greater scale, with higher precision, and at lower cost. Many capabilities that once required skilled hackers can now be performed by individuals with much less technical expertise. For OT environments, this compresses the time defenders must detect and contain an intrusion before it affects pumps, chemical dosing, pressure, filtration or wastewater processes. The problem is especially acute for small and rural utilities. Attackers can increasingly automate their work, while many utilities still depend on aging control systems, shared passwords, remote-access tools, understaffed IT teams, and vendors that may not provide continuous monitoring. AI therefore risks creating a systemic disparity where attackers leverage automated orchestration while defenders rely on legacy, tailored responses. Below are a few ways AI is changing the water and wastewater sector threat landscape, to include acceleration and automation of traditional threats to the rising impact of agentic AI. Conversely, AI can assist organizations in proactively identifying network and systems anomalies and automating incident response. Before deploying AI-based cyber defense platforms, water and wastewater utilities should be mindful of certain challenges outlined below.

How AI is Changing the Water and Wastewater Sector Threat Landscape

AI Lowers the Barrier to Entry

Generative AI can help relatively inexperienced actors create convincing phishing messages, translate them into multiple languages, develop scripts, interpret technical documentation and troubleshoot failed

Continues on page 2

attacks. The UK National Cyber Security Centre (NCSC) assesses that AI will increase the scale, speed and effectiveness of existing attack methods and expand the population of actors capable of conducting cyber operations. For a water utility, that can mean more credible emails impersonating utility managers, engineering firms, equipment vendors or state regulators. It can also enable automated password spraying and credential-stuffing campaigns, and better-written malware and scripts, although human expertise is still generally required for sophisticated OT manipulation.

AI Accelerates Reconnaissance

Attackers can use AI to correlate information from internet-exposed devices, vendor manuals, procurement records, professional profiles, leaked credentials, and vulnerability databases. This makes it easier to identify the water utility's supervisory control and data acquisition (SCADA) or human-machine-interface vendor, remote-access products in use, network architecture, employees with privileged access, default or commonly reused credentials, and known vulnerabilities affecting specific OT devices. Also, AI is particularly useful for summarizing lengthy technical manuals and explaining unfamiliar industrial protocols. This does not automatically give an attacker deep process-engineering expertise, but it reduces the time needed to understand a target.

AI Shortens the Vulnerability-Exploitation Window

AI-assisted vulnerability research can help attackers identify vulnerable code, develop proof-of-concept exploits and adapt existing exploits to new targets. The NCSC further warns that AI is likely to further reduce the already-short period between public disclosure of a vulnerability and active exploitation. This is perilous for OT because patching is normally slower than in enterprise IT. Utilities may need vendor approval, operational testing, planned outages or regulatory coordination before modifying a control system. Some devices cannot be patched at all without replacement.

AI Improves Social Engineering and Impersonation

According to the EC-Council University, generative AI enables attackers to mimic natural human language flawlessly, analyze publicly available data to personalize messages, and adapt conversations in real-time. Voice cloning, synthetic video and AI-generated text can be used to impersonate water utilities' executives, equipment vendors, regulatory agencies, and managed service providers.

AI Increases Ransomware Efficiency

A recent article published by Businesswise, ransomware activity continued to climb in the second quarter of 2026 as threat actors increasingly use AI as a productivity enabler. Ransomware groups can use AI to

automate victim research, phishing, data classification, extortion messaging and analysis of stolen files. AI can also help criminals identify documents that would create the greatest regulatory, operational or reputational pressure.

Water utilities are particularly sensitive to downtime. Even when ransomware affects only business systems, utilities may lose access to billing, laboratory data, work orders, maintenance records, mapping systems, email and vendor support. If IT and OT are poorly segmented, the disruption can spread toward operations.

AI Can Support OT-Specific Targeting

More capable actors can use AI to analyze process data, alarm histories, engineering files and control logic after gaining access. Also, AI can help attackers find the unique digital codes (tags) for pumps, valves, or chemical systems, which would enable attackers gain the ability to manipulate physical infrastructure. This is critical because it bridges the gap between a digital intrusion and real-world effects. However, the risk should not be overstated, manipulating OT environments still requires process knowledge, access and testing. Notwithstanding, AI can accelerate the attacker's learning after intrusion.

Leveraging AI to Defend OT and IT Environments in the Water and Wastewater Sector

AI has the potential to transform the defense posture of the water and wastewater sectors from a reactive model—responding only after a failure or cyber attack—to a predictive and autonomous model that continuously detects anomalies, prioritizes risks, and accelerates response. This is particularly important as water and wastewater utilities face increasing cyber threats from nation-state actors while simultaneously struggling with aging infrastructure and limited cybersecurity staffing.

AI for Continuous Threat Detection

AI can analyze millions of events from IT and OT environments simultaneously, identifying subtle

indicators that traditional rule-based monitoring often misses. According to NIST IR 8596 (Initial Preliminary Draft), "AI improves monitoring and strengthens threat detection by flagging anomalies, correlating suspicious behaviors, and spotting unusual patterns faster than humans and other automated tools." Unlike traditional signature-based detection, machine learning establishes a baseline of "normal" operations and flags deviations in real time, even if the attack has never been seen before. This significantly reduces detection time and helps uncover sophisticated attacks. Examples of areas of cyber defense where AI can assist include detecting abnormal operator logins or privilege escalation, identifying unusual PLC or SCADA commands; recognizing deviations in pump, valve, and chemical dosing behavior; correlating cyber events with physical process changes and detecting insider threats through behavioral analytics.

AI-Driven Sensor Analytics

Modern water systems already collect enormous amounts of telemetry from a variety of systems and sensors. AI models can continuously analyze these data streams to detect water main leaks, equipment degradation, pump failures, unauthorized valve operations, chemical dosing anomalies, and sensor manipulation caused by cyber attacks, aging equipment, or other causes. Instead of waiting for alarms to exceed fixed thresholds, AI identifies subtle patterns that often precede failures by hours or days.

AI-Assisted Incident Response

During an active cyber incident, AI can dramatically reduce response time by automatically correlating security alerts, identifying the likely attack path, determining affected assets, recommending containment actions, generating incident timelines, and producing regulatory reporting documentation. For example, if ransomware reaches an engineering workstation connected to SCADA, AI can rapidly identify impacted PLCs, recommend network isolation, prioritize recovery, and generate reports for leadership and regulators. EPA, CISA, and the FBI emphasize the importance of rapid detection, coordinated response, and practiced incident response plans for water utilities.

Challenges for AI-based Cyber Defense Platforms

Despite its promise, AI also introduces new risks. For instance, AI models can be manipulated through adversarial attacks. Also, poor-quality sensor data can lead to inaccurate recommendations. Moreover, generative AI systems may hallucinate (false, fabricated, or misleading information that is presented as a fact) or provide unsafe operational advice. Other considerations include OT environments often lack sufficient historical data for training, small and rural water and wastewater utilities frequently lack AI and cybersecurity expertise, and AI systems themselves become attractive targets for attackers.

Recommendations for the Water and Wastewater Sector to Maximize the Value of AI

Utilities can maximize the value of AI by:

- Integrating AI with SIEM, SOAR, EDR/XDR, and SCADA monitoring.
- Deploying AI-based anomaly detection across both IT and OT networks.
- Building digital twins to support incident planning and operator training.
- Using AI to prioritize vulnerabilities based on operational risk.
- Leveraging AI-assisted threat intelligence from government and commercial sources.
- Maintaining human approval for safety-critical operational actions.
- Aligning AI deployments with the NIST Cybersecurity Framework 2.0 and sector-specific guidance from EPA and CISA (add links?).

Additionally, in May, CISA and other agencies published guidance "Careful Adoption of Agentic AI Services," outlining the security risks and best practices associated with adopting agentic AI systems. The guidance highlights how agentic AI, which is capable of autonomous decision-making and action, introduces increased attack surface and risk of misuse. It recommends integrating AI risk management into existing cybersecurity frameworks; limiting agent privileges; and ensuring strong oversight, monitoring, and control throughout the AI lifecycle.

As agentic AI becomes more integrated into critical infrastructure environments, its autonomy and access to systems introduce new pathways for exploitation and operational risk. Organizations adopting these technologies benefit from aligning AI deployments with existing cybersecurity practices, emphasizing least privilege, segmentation, and continuous monitoring. Careful implementation and oversight are key to ensuring these systems enhance efficiency without introducing unintended security gaps.

Additional Reading:

- Anthropic Releases Claude Fable 5: Mythos-Class AI Signals a New Phase in Vulnerability Management
- SANS - AI Security Maturity Model™ eBook
- JADEPUFFER: Agentic ransomware for automated database extortion

ASK THE EXPERT: Interview with Three Water Utility IT Directors

The cybersecurity threat landscape facing water and wastewater utilities is rapidly evolving, with emerging technologies, such as AI, altering threat actor tactics and offering new methods for vulnerability exploitation. These dynamics are coupled with increasing geopolitical tensions, which all together play a role in the evolution of this complex threat environment.

Furthermore, operators and network defenders must balance daily operational requirements with legacy systems, resource constraints, and an expanded attack surface. To help us understand these issues and methods to mitigate them, we spoke with Bryon Black (BB), IT Manager for the South Coast Water District (CA); Patrick Bruner (PB), IT Director at Des Moines Water Works (IA); and John Sobieralski (JS), IT Director with the City of Aspen (CO).

Q: Threat landscape - What kinds of cyber threats have you seen targeting water and wastewater utilities, and how has that changed over the past few years?

BB: Threats now are significantly more frequent and often appear to be emanating from organized attack vectors. We see many "door knocks, and window rattles", often in the realm of millions in a week. The other major area is software / hardware supply chain, where software libraries / components, or hardware components are being compromised, which is often well outside of a utilities' scope to control. AI is driving some of this with Anthropic type models that can pull out dormant or not easily found exploits.

PB: The volume is what's really changed. Most of what we see is automated and hitting everybody at once rather than aimed at us specifically, so a ten-person shop like mine deals with the same constant probing and phishing that a big utility does. Ransomware is still what I worry about most. The part that's hardest to get your arms around is the vendor and software supply chain, where something gets compromised upstream in a product you bought and trusted, well before it ever reaches you.

JS: The threats we see are basically the same as always, just coming more frequently now due to AI automation. Attempts to compromise identity and gain VPN access, as well as attempts to compromise external firewalls through vulnerabilities are the most prevalent. Compromising any openly available OT devices and compromise of a vendor's software supply chain are the more recent threats for all critical sectors. Supply chain risk is the hardest to mitigate as you don't really know if the new software or update code has been vetted by the vendor.

Q: IT/OT convergence – How do you approach securing the boundary between IT networks and operational technology (SCADA, PLCs, HMIs) without disrupting plant operations?

BB: This required significant investment and buy-in from both IT and OT staff, as well as rearchitecting of our IT (cybersecurity) approach, revamping and better isolating our OT architecture. We also deployed protective systems from the IT side to help monitor the OT side leveraging DMZ access to the OT. This gives our OT and IT staff visibility across the two platforms yet keeps both relatively sterile.

PB: For us this is as much about who owns what as it is about the technology. Water production owns the OT and SCADA side, IT owns the enterprise, and we've agreed on where the line between them sits instead of leaving it fuzzy. IT provides monitoring and visibility but doesn't reach into the control systems, and when we pen test the OT side, that's led on their end under the SCADA plan. What keeps plant operations from getting disrupted is pretty simple: nothing crosses that boundary without both teams at the table.

JS: We are fortunate in that we are relatively small and our IT and OT networks are completely separate. Typical IT enterprise apps such as email, office apps, internet browsing, ERP, etc. are on separate user PCs on a separate city network. OT devices, engineering PCs, SCADA, and human-machine interface (HMI) servers are on their own network. Remote access to the OT network is only allowed through approved individually issued devices, not their city PCs.

Q: Incident response - Can you walk through what your incident response plan looks like for a suspected breach, and what utilities that don't have a mature plan yet should prioritize first?

BB: Our plan has evolved over a couple of years from a list of vendors and key points to contact to a workable playbook for dealing with cyber events on either IT or OT systems as well as dealing with cyber insurance claims. The plan has been reinforced with a rigorous testing program for our enterprise and OT backup systems, where we test our ability to recover from backup / archive on a quarterly basis and we report on the results. Our thinking is we can thwart a large ransom payout if we have really good, known quantity backups, even if the bad guys get a foot hold. We also hold quarterly briefings to discuss and enhance the CIRP. The plan is a part of our annual strategic goals.

PB: Our incident response plan is a real working document now, we're on version 3.1, and it sits on top of a disaster recovery plan and a business impact analysis that tells us which systems have to come back first. If you're a utility just getting started, I'd do three things in this order. Figure out your critical assets through a BIA so you're not guessing in the middle of a crisis. Prove you can actually restore from backup, because a backup job reporting success isn't the same as knowing you can recover. And write down who you call, including your cyber insurance contacts, before the day you need them. If you've got backups you trust, you've taken away most of the leverage a ransom attack has over you.

JS: As is typical for small utilities, ours isn't as developed as it should be for a suspected cyber incident. Every station has information posted as to who to call and what to report, which is very basic IR. What we do have are good step by step procedures for shifting everything to fully manual operations, once any automated failures occur or it's determined that is what has to take place. These procedures have been tested and practiced though not on a regular basis. There are good backups both on-prem and off-site. As a small utility developing a better written IR plan that integrates cyber with manual continuity of operations and recovery processes and then having regular tabletop scenarios are the next steps.

Q: Workforce and culture - How do you build a security-conscious culture among operations staff who may see cybersecurity as "IT's job" rather than part of their daily responsibilities?

BB: We started with monthly training, delivered online (ex. Beyond Trust), we do quarterly phishing tests, results from the test drive the next round of training. More recently we have changed our narrative from cyber risks are something that might occur or it might affect operations or operations staff, to everyone is now in the involved. All of us are prime targets of the now highly organized crime syndicates that are running cyber incidents as a for profit business. This changes the narrative with operations staff, combined with the millions of door knocks and window rattles, and the possibility that a breach could cost the agency millions of dollars their attention to the risks have evolved.

PB: We run role-based security awareness training and regular phishing tests, and what people click on drives what we train on next. The bigger thing for us is how we talk about it. I'd rather give people a safe way to do their job than hand them a list of things they can't do, so the training is built around enabling them. And I try to connect it to the mission. A breach here puts water service for 600,000 people at risk, and operations staff hear that a lot differently than they hear a policy reminder.

JS: We have quarterly security awareness trainings and additional role-based training (ICS related) for the utilities side as well as monthly phishing tests. Operations staff gets briefed on CISA/FBI relevant bulletins and have discussions when a utility's cyber incident eventually becomes public. The trick has been to change their perspective on who is responsible for security. This has evolved over time to where the OT teams now have a good understanding that security is part of their job as well.

Q: Resource constraints - Many smaller utilities lack dedicated cybersecurity staff or budget. What are the highest-impact, lowest-cost steps a resource-strapped utility can take to meaningfully reduce risk?

BB: Lowest cost, protective DNS (Domain Name System), at least that will reduce the risk of having an exploit contact the exploits command and control. That could easily save a lot of pain. Work to paint a narrative of what it costs to do nothing. Boards and decision makers will likely have a different view of what an incident costs if they are able to quantitatively weigh what investing in protective cyber security measures will cost versus doing nothing and suffering a breach. Use the EAL (Estimated Annual Loss) metric to illustrate what it costs to do nothing and get breached, versus actually investing in legitimate cyber protections and perhaps avoid being breached. The metric is calculated for both doing nothing and calculated for a well-supported cyber protection program.

- **EAL =** {Annualized Rate of Occurrence (ARO) X Loss Magnitude (LM)}
- **ARO (Annualized Rate of Occurrence):** The estimated probability or frequency of a threat event happening in a given year (e.g., a probability of 0.2 means once every 5 years).
- **Loss Magnitude (LM):** The total financial cost incurred if the event successfully occurs (including recovery, downtime, and response costs).

Continues on page 6

- **Key Purpose:** EAL translates technical vulnerabilities and abstract risks into concrete dollar amounts, allowing organizations to justify the ROI of protective systems and security spending.

PB: Start with the cheap controls that stop the most damage: MFA, protective DNS, backups you've actually tested, phishing-based training, and a written incident response plan. Beyond that, the most useful move for a small team is leaning on a framework and some outside help instead of trying to hire your way there. Running on NIST CSF with a part-time vCISO gives my ten people the structure a much bigger security team would have. And learn to talk about risks in dollars with your board. Decision-makers fund this differently once they can see the cost of doing nothing next to the cost of protecting against it.

JS: Some quick wins: change all factory default credentials, maintain and test offline backups, protective DNS (DNS filtering), enable MFA, have a basic IR plan with steps for full manual operations, and disconnect any OT from public internet access. Some of these may be more difficult than others to implement but start by contacting other nearby utilities you have relationships with to ask for help. Join WaterISAC! I agree with Bryon and Patrick that you have to learn how to explain the risk in dollars to your board or city leadership to get the funding that is needed.

WaterISAC Advisory – Safeguarding Sensitive Operational Information

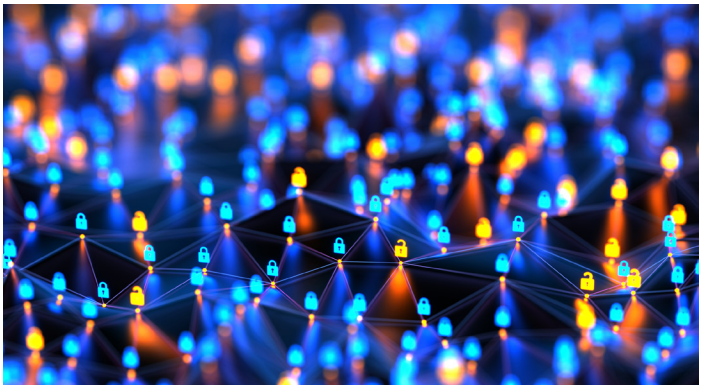
AWWA and WaterISAC advise water and wastewater systems to closely safeguard sensitive operational information following multiple public records requests from AI service providers.

While it is unclear how the data would be used, in one case, an AI service provider appeared to have direct knowledge of the data historian used by the utility and specifically asked for "all SCADA logs for 2026 for all treatment, distribution and wastewater management systems." In addition, the requestor(s) added that they were seeking "daily or hourly historical logs for the following environmental and physical process indicators only:

- Inflow and outflow water volumes/flow rates (MGD).
- Aggregate water quality baseline metrics (e.g., daily average turbidity, pH, dissolved oxygen, and conductivity).
- Historical reservoir/tank storage elevations or percentage capacity levels.
- Aggregate daily energy consumption or equipment run-times (e.g., daily total pump hours), without any active electrical load telemetry."

This information has obvious operational sensitivity, providing key details about system performance. Utilities should be aware that while individual data requests may appear benign, the aggregation of operational data across multiple systems has the potential to reveal patterns, vulnerabilities, and system behaviors. Such operational data could be used maliciously to threaten continuity of service, which could harm the public and national security interests.

AWWA prepared a report in 2019, ***Protecting the Water Sector's Critical Infrastructure Information***,



which summarizes each state's information disclosure exemptions that can be used by a water system to protect sensitive information. It is best practice for utilities to carefully consider the potential sensitivity of the information being requested and make a risk-informed decision on whether, and under what conditions, to respond in compliance with applicable state information protection laws.

AWWA and WaterISAC encourage water and wastewater systems to closely review public record requests, such as the one described, to ensure their interests are not compromised. Water and wastewater systems should also review disclosure protections under current state law with legal counsel.

WaterISAC encourages utilities with concerns or having received similar requests to share that information with its analysts for tracking. Likewise, **Kevin Morley**, federal relations manager at AWWA, invites utilities to contact him, with questions.

*Contact WaterISAC **via this link here** with any questions or concerns.*

CISA Issues Alert Urging Water and Wastewater Utilities to Protect OT Against Activity Targeting PLCs

On July 30, CISA issued an alert warning of a significant increase in cyber threat actors targeting PLCs in the water and wastewater sector. CISA noted attackers accessed internet-exposed PLCs, modified passwords to lock out operators, and changed device IP addresses to disconnect the controllers. This has led to boil water notices and forced utilities into sustained manual operations.

CISA notes the targeting spans water entities of all sizes, including organizations with mature cybersecurity programs. Of particular concern, the exposed assets include cellular modems installed by operators, vendors, or system integrators that may not be documented or captured in routine attack surface scans. CISA further notes internet-exposed OT carries elevated risk of defacement, unauthorized configuration changes, operational disruption, and, in severe cases, physical damage.

WaterISAC and EPA strongly urge utilities to review and follow CISA's alert and recommendations without delay:

- Disconnect the PLC from the internet. Remote access for operational purposes should go through a VPN or gateway device, not directly to the PLC.
- Enable password protection and change default passwords.
- Allow list IPs to only allow remote access from known engineering laptops or other critical OT assets.
- Once PLCs are disconnected from the public internet, operators should ensure a known-clean backup of the PLC image exists in case operators are locked out by a modified password.
    - It may be necessary for utilities to contact their integrators for assistance and to make sure the utility maintains a backup copy in a secure location (the integrator should not be the only one with a copy of PLC code and backups).

To securely enable remote access to your OT systems, CISA recommends system owners, operators, and integrators see the following resources for guidance:

- CISA: Primary Mitigations to Reduce Cyber Threats to Operational Technology
- United Kingdom's NCSC: Secure Connectivity Principles for Operational Technology
- FBI: Malicious Cyber Actors Targeting Water and Wastewater Sector Internet Facing Programmable Logic Controllers, Causing Operational Disruptions

In addition to the CISA alert, the FBI noted that across multiple victims, similar network configurations supplied by third parties may give malicious cyber actors a chance to increase their success when vulnerable network and hardware setups are shared by customers. **Utilities should therefore proactively contact integrators, service providers, and other vendors supporting critical OT systems; share this alert if they are not already aware of it and *take any necessary follow-up actions*.**

Read CISA's full alert here.

Additional Reading:

- Review of the July 2026 Cyberattacks Against U.S. Water and Wastewater Systems
- At least 12 states report cyberattacks on water systems possibly linked to Iran-backed hackers, sources say

Drones – The Next Generation of Physical Security Threats Facing Water and Wastewater Utilities

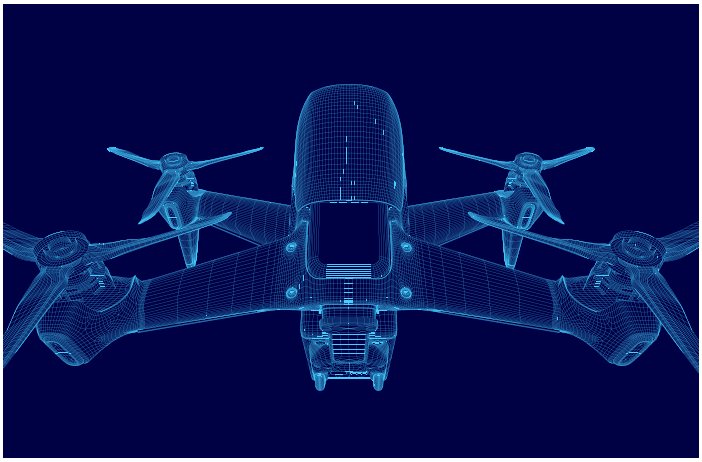
Water and wastewater utilities continue to regularly experience unauthorized drone overflights and find drones on their property. Criminals have also used drones to specifically target utilities. And more nefariously, a range of threat actors are increasingly utilizing drones for violent acts. In 2024, the FBI arrested a domestic violent extremist (DVE) for plotting to blow up a Nashville electric substation with an explosive-laden drone to further his ideological goals. In the same year, authorities arrested a teenager in Arizona, who was inspired by the Islamic State, for planning to use an explosive-laden drone against a Phoenix Pride event.

Indeed, in last year's Annual Homeland Security Week Conference, several vendors marketed drone detection and anti-drone technologies designed to target an incoming drone and stop it from entering the facility's airspace. At the time, there were concerns that even relatively small, inexpensive drones could carry explosive charges capable of causing significant damage to sensitive equipment at critical infrastructure sites.

Fast forward to May of this year, former CIA Director David Petraeus observed of the U.S.-Iran war that "autonomous drones can form swarms that can overwhelm defenses through large numbers while adapting to changing battlefield conditions by communicating with one another, instead of being remotely piloted by a human controller…That gets really, really, really scary, actually, because autonomous systems mean … you're not limited by the number of pilots that you have who are remotely flying these systems."

Subsequently, Chinese researchers recently published a peer-reviewed algorithm —Heterogeneous Graph Spatio-Temporal Reasoning (HG-STR) — reportedly enabling fixed-wing drone swarms to autonomously identify, track and engage targets in simulation even when communications are fully jammed and sensor visibility is degraded. Despite the potential future threat of a hostile nation state, such as China, employing an autonomous drone swarm against U.S. targets, the primary near-term risk is downstream migration of autonomous swarm concepts to non-state actors via commercial platforms.

In late April, for instance, al-Qaida-affiliated Jama'at Nusrat al-Islam wal-Muslimin (JNIM) and the separatist Tuareg-led movement Azawad Liberation Front (FLA) demonstrated the use of individually operated one-way attack drones in combined air-ground operations. The combined attacks drove Mali's military and Russian troops from multiple towns and killed Mali's Defense Minister.



Autonomous and drone swarm technologies might primarily be the purview of the military. However, with the growth of cellphone-based AI tools and swarms of armed drones costing perhaps a few thousand dollars each, these threats are not far in the distant future.

What Can I Do to Protect my Water or Wastewater Utility against the Growing Drone Threat?

Earlier this year, the U.S. Department of War published a guidance product, "JIATF 401 Guide for Physical Protection of Critical Infrastructure." The guidance is designed to help military commanders and law enforcement use passive measures to secure vital critical infrastructure against threats from small unmanned aircraft systems (sUASs), or drones.

The report emphasizes that due to the growing drone threat, "individuals outside a facility, with no intent to gain access, can surveil or threaten facilities and events from significant stand-off distances. Security is no longer defined solely by who gets in, but by how effectively threats from outside the facility are mitigated." Because of this shift, "local authorities [need] to think about physical protection in new ways that include solutions that are layered, outward-looking, and focused on denying access, visibility, and opportunity, well beyond the entry gate or perimeter."

A central concept of the guide is the "Harden, Obscure, Perimeter" framework, a methodology focused on shaping the physical environment to counter drone threats. This approach emphasizes practical, layered solutions that can be implemented without the need to procure and deploy expensive technological counter measures. According to the guide, "hardening involves creating physical obstacles to sUAS flight, such as netting or structural shielding. Obscuring focuses on reducing a drone's ability to identify and access critical assets through measures like visual clutter and

temporary barriers. The perimeter aspect extends security well beyond the traditional fenceline, creating layered defenses to detect and deter threats before they reach the intended objective."

In short, EPA and WaterISAC highly encourage water and wastewater utilities to assess what parts of their facility would be vulnerable if a small explosive-laden drone targeted their operational equipment. This is today's threat. Tomorrow's threat could be a half-dozen inexpensive armed drones, operating in coordination and autonomously-AI-driven to carry out the malicious goals of someone who just spent $20,000 on the whole system.

Additional Reading:

- Asymmetric Warfare in the Drone Age: Lessons from Ukraine and an Urgent Warning for U.S. Critical Infrastructure
- U.S. Federal Government Issues New Rule Allowing Local Law Enforcement to Take Down Drones
- FAA Extension, Safety, and Security Act of 2016 – Section 2209 Notice of Proposed Rulemaking

Mitigation Recommendations:

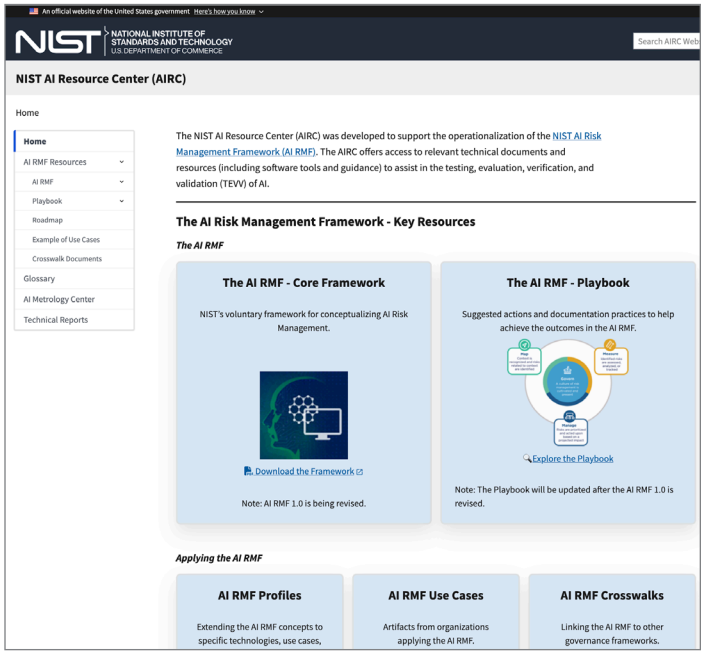
- CISA – Be Air Aware
- (TLP:CLEAR) CISA Releases Three Unmanned Aircraft Systems (UAS) Security Guidance Products
- CISA – Suspicious UAS Identification Poster and Postcard

EPA's Office of Water Emergency Response and Cybersecurity – NIST's AI Security Resources

EPA's Office of Water Emergency Response and Cybersecurity, (OWERC) provides free tools, training, and no-cost technical assistance to help drinking water, wastewater, and stormwater utilities strengthen their physical security and cyber resilience against natural and man-made threats. In regard to AI security, OWERC recommends that water and wastewater utilities use the NIST AI Resource Center (AIRC)

The NIST AIRC supports implementation of the NIST AI Risk Management Framework by providing guidance, tools, and best practices for managing AI risks throughout the AI lifecycle. EPA's Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems references the NIST AI RMF as a resource for organizations using AI in cybersecurity and risk management, making the AIRC a useful companion resource for water and wastewater utilities.

- *Access NIST AI Resource Center here.*
- *Access EPA OWERC's security and resilience resources here.*



INSIDER THREAT CORNER – AI Impacts to Insider Threats for the Water and Wastewater Sector

With the advent of AI, coupled with increased remote access given to contractors and other third-parties for operational activities, water and wastewater utilities are increasingly at risk of succumbing to compromise driven by insider threats. In a recent report, cybersecurity firm Dragos documented the first known AI-assisted cyberattack on water utility infrastructure worldwide, when an intrusion campaign targeted a Mexican water utility.

Drinking water utilities that serve more than 26 million Americans were found to carry critical or high-risk cybersecurity vulnerabilities, according to an EPA Office of Inspector General report. This risk could lead to many unintentional insider threats. When water sector employees or contractors do not take appropriate measures to enhance cybersecurity, it could lead to compromise and disruptions. AI significantly amplifies insider threat vulnerabilities in the water sector by automating reconnaissance, generating sophisticated malicious code, and accelerating the exploitation of OT networks. Insiders can inadvertently expose proprietary infrastructure or use these tools maliciously to bypass traditional air-gapped security measures.

The integration of AI alters the insider threat landscape for water utilities across several critical areas:

1. AI-assisted intrusion and code generation: adversaries and compromised insiders utilize models like Claude and GPT to traverse codebases, write malicious scripts targeting industrial control systems, and map access pathways to OT environments. This means an insider with lower technical skills can cause systemic damage using AI-generated attack paths.
2. Physical disruption via SCADA systems: Insiders who have legitimate access to SCADA systems can manipulate chemical feeds, disable water quality monitors, or cause sewage overflows. The integration of AI tools allows malicious insiders to obscure these actions from monitoring screens or automate sabotage.
3. The rise of agentic AI introduces new vulnerabilities where automated bots seek out unauthorized access, search internal repositories, and connect to third-party domains without permission. Agentic AI is capable of understanding goals and reason and can take autonomous actions to complete complex tasks without constant human intervention.

4. Supply chain and third-party risks: The water sector faces significant supply chain risk when third-party vendors incorporate AI into their products or services, as utilities often lack visibility into how that AI was developed, trained, or vetted before it reaches them. This opacity creates an opportunity for malicious code or compromised components to be embedded in AI systems earlier in the supply chain—before the vendor ever installs or deploys the solution at the utility—potentially giving adversaries a foothold in critical OT environments.

Additional Reading:

- AI in the Breach: How an Adversary Leveraged AI to Target a Water Utility's OT
- Third-Party Risk Management – Evaluating Cyber Risk Posed by IT and Managed Service Providers
- CISA - Insider Threat Mitigation Guide

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 and Operations Coordination | www.epa.gov/national-security
- Drinking Water and Wastewater Resilience Website | www.epa.gov/waterresilience
- Cybersecurity for the Water Sector | https://www.epa.gov/cyberwater

Water Sector Coordinating Council

- American Water Works Association (AWWA)
- Association of Metropolitan Water Agencies (AMWA)
- National Association of Clean Water Agencies (NACWA)
- National Association of Water Companies (NAWC)
- National Rural Water Association (NRWA)
- Water Environment Federation (WEF)
- WaterISAC
- Water Research Foundation (WRF)