OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
16 JULY 2025 DHS-IA-IF-2025-17585

CYBERSECURITY

(U//FOUO) Insider Threats Pose Significant Threat to Water and Wastewater Systems

(U//FOUO) ***Scope Note:*** *This assessment answers a question from the Environmental Protection Agency, which is the Water and Wastewater Systems Sector's Sector Risk Management Agency, related to insider threats to this critical infrastructure sector.*

(U//FOUO) **In recent years, insiders—often disgruntled current or former utility employees—have conducted physical and cyber attacks against US water and wastewater infrastructure systems with varying degrees of impact, and they pose a risk of significant harm to the sector.** While insider threats are not unique to this sector and the number of reported incidents remains low, recent high-profile examples of insider threat activity demonstrate that it is a persistent and potentially high-impact threat. Insider manipulation or disruption of water and wastewater systems (WWS) could have severe implications to civilian health and safety, as well as affect interdependent infrastructure sectors and government and business functions.

- (U//FOUO) The US WWS Sector is vulnerable to cyber intrusions by maliciously motivated current or former employees who maintain active credentials, whether properly or improperly. Malicious insiders have exploited privileged access to disable water treatment system safeguards and disinfection processes, endangering public drinking water supplies, according to DOJ indictments. The sector's shift to remote management and digital operational technology makes site management more efficient and convenient but could also enable a knowledgeable insider to have a considerable impact on operations.
- (U//FOUO) Unintentional actions by employees can also pose risks to the US WWS Sector. In 2021, an employee at a water treatment plant in Florida inadvertently clicked on incorrect buttons, creating the illusion of a malicious actor gaining remote access to operational controls, according to industry reporting. While the operator was able to correct the mistake quickly and there was no impact to operations, the confusion led to scrutiny of the sector and a federal investigation, according to the same source.

- *(U//FOUO)* Insiders can use their knowledge and access to facilities to conduct physical sabotage or vandalize equipment. In 2022, a disgruntled employee of a water department in Massachusetts entered a pumping station and tampered with chlorine controls, resulting in insufficiently disinfected water being introduced into the drinking water system, according to DOJ and press reporting. The insider disabled an alarm that would have alerted employees to the low chlorine levels, but other employees were able to respond before chlorine levels became dangerous.

(U//FOUO) **Insider threats likely exploit facility or technology access management shortfalls, highlighting mitigation opportunities for US WWS Sector entities.** Enhanced cyber hygiene and physical access practices—especially in the case of an employee's departure—and insider threat awareness training could reduce opportunities for insider threat actors to take malicious actions against the sector.

- *(U//FOUO)* Implementing basic cybersecurity measures—such as promptly revoking former employees' network access and enforcing strong password policies—can help sector owners and operators mitigate threats from insiders, according to a CISA and NSA identity and access management guide.[a] User activity monitoring would also allow WWS utilities to detect other technical indicators of compromise from insider threat actors, such as unauthorized attempts to escalate permissions or privileges, an unauthorized device connected to the network, and attempts to access resources not associated with the individual's normal role, according to a separate CISA guide on insider threats.[b]
- *(U//FOUO)* Some threat actors also pose as employees to conduct malicious activity, which can be mitigated by training employees to report suspicious behavior and verify access to restricted areas. In August 2024, an individual impersonating a state government employee trespassed into a water treatment facility in California by cutting a padlock; the individual then tampered with chlorine pumping systems and attempted to gain access to chlorine and fluoride storage sheds. The intruder promptly departed the facility after being challenged to show identification.

[a] *(U)* The CISA/NSA Recommended Best Practices for Administrators: Identity and Access Management Guide can be accessed at https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management.
[b] *(U)* The CISA Insider Threat Mitigation Guide can be accessed at https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide.

(U) Insider Threat and Access Management Resources

(U) CISA regularly publishes open-source resources and provides services to assist network defenders and critical infrastructure owners and operators with identifying and mitigating against vulnerabilities and malicious activity.

- (U) CISA Guide, "Insider Threat Mitigation Guide," dated November 2020.
- (U) CISA/NSA Guide, "Recommended Best Practices for Administrators: Identity and Access Management," dated March 2023.

(U) The National Insider Threat Task Force in ODNI's National Counterintelligence and Security Center (NCSC) publishes unclassified guides and resources, primarily for federal agencies, that are applicable to state, local, tribal, and territorial partners and industry partners, to address all insider threats.

- (U) NCSC guide, "Insider Threat Mitigation For U.S. Critical Infrastructure Entities," dated September 2024.[c]

[c] (U) The ODNI's NCSC "Insider Threat Mitigation for US Critical Infrastructure Entities" guide can be accessed at https://www.dni.gov/files/NCSC/documents/nittf/20240926_Insider-Threat-Mitigation-for-US-Critical-Infrastructure.pdf.

Reference and Dissemination Information

Feedback	*(U//FOUO)* Customers may submit feedback on DHS I&A Analytic products via the DHS I&A Evaluation Form located at the following addresses: • Unclassified: https://forms.office.com/g/FKkyksC3eg • SIPR / HSDN: https://go.sgov.gov/IAFeedback • JWICS / CLAN: https://go.intelink.ic.gov/IAFeedback
Definitions	*(U)* **Insider Threat:** An insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization and its data, personnel, facilities, and associated resources.
Reporting Suspicious Activity	*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi. *(U)* **To report a computer security incident, please contact CISA at 888-282-0870; or go to IRF Index - IRF. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* **To report this incident to the Intelligence Community, please contact your DHS I&A Field Intelligence Officer at your state or major urban area fusion center, or e-mail IA-P-FID-ALL-HQS@hq.dhs.gov.** DHS I&A Field Intelligence Officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Warning Notices & Handling Caveats	*(U)* **Warning:** This information is provided only for intelligence purposes. It cannot be used in connection with any foreign or domestic court proceedings or for any other legal, judicial, or administrative purposes. *(U)* **Warning**: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security official without further approval from DHS.

	(U) All US person information has been minimized. Should you require US person information, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.