TLP:CLEAR

Q2 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

- Third-Party Risk in the Water and Wastewater Sector
- Ask the Expert: Interview with DC Water's Director of Security
- Iranian Cyber Threat to U.S. Water and Wastewater Utilities Amid the Conflict with Iran
- Iran Physical Security Threats and Supply Chain Disruptions Stemming from the Conflict
- The 2026 National Cybersecurity Drill, "A Day Without SCADA," on July 8 at 1:00 PM ET
- Insider Threat Corner – Third-Party Risk

Third-Party Risk in the Water and Wastewater Sector

Water and wastewater utilities increasingly rely on third-party vendors to support core business and operational functions, including software management, remote access solutions, billing platforms, and industrial control system (ICS) maintenance. While these partnerships enable utilities to enhance efficiency and leverage specialized expertise, they also introduce significant cybersecurity risk. Third-party vendors often maintain privileged access to utility networks and operational environments, creating potential pathways for adversaries to bypass perimeter defenses and gain a foothold within critical systems. As a result, third-party risk should be viewed not as an external concern, but as an extension of a utility's internal threat landscape.

The interconnected nature of modern water systems amplifies this risk. Many utilities operate within hybrid IT/OT environments, where trusted vendor connections bridge business IT networks and operational technology. If a vendor's credentials are compromised, or if their software is exploited, adversaries can leverage these trusted relationships to move laterally within utility systems. A recent case study highlighted in a prior EPA–WaterISAC bulletin described a cyber incident affecting multiple water utilities in Texas, where a commonly used third-party remote access solution was identified as a potential access vector for threat actors attempting to manipulate water tower operations. Although the impact was mitigated through rapid response, the incident underscores how a single vendor vulnerability can have sector-wide implications.

Beyond direct cyber exploitation, third-party dependencies also introduce risk tied to supply chain interdependencies. Supply chains for critical infrastructure components (including pumps, sensors, and control systems) are often complex

and internationally sourced, creating opportunities for disruption, manipulation, or the introduction of insecure technologies. Additionally, third-party contractors can create physical security risks to water and wastewater utilities (see the insider threat corner below). For example, unsecured materials at a utility construction site managed by a third-party contractor could attract financially motivated criminals seeking to breach the site and steal valuable equipment.

In a sector where continuous operations are essential to public health and safety, even minor disruptions in vendor services or product integrity can cascade into broader operational impacts, affecting water quality, service delivery, and public confidence.

Third-Party Risk Management: Mitigation Actions for Utilities

To effectively manage third-party risk, this report's

Continues on page 2

authors encourage water and wastewater utilities to implement a structured, lifecycle-based approach that addresses vendor relationships from initial onboarding through ongoing operations. Key actions include:

Conduct thorough vendor due diligence prior to onboarding, including:

- Evaluating vendor cybersecurity practices and maturity.
- Assessing access requirements (IT, OT, remote access, data handling).
- Identifying operational dependencies and potential single points of failure.

Establish clear contractual cybersecurity requirements, such as:

- Establishing mandatory incident reporting timelines and procedures.
- Adhering to recognized cybersecurity standards and best practices.
- Defining roles and responsibilities for security across both parties.

Enforce the principle of least privilege for all third-party access:

- Limiting vendor access strictly to necessary systems and data.
- Restricting access duration and scope based on operational need.
- Regularly reviewing and revoking unnecessary permissions.

Strengthening third-party risk management is essential to safeguarding the resilience of the water and wastewater sector. As threat actors increasingly target supply chains and trusted relationships, a utility's security posture is only as strong as its vendors. By integrating third-party risk into broader cybersecurity strategies, utilities can better protect critical infrastructure, maintain continuity of operations, and uphold public trust in the delivery of essential services.

Helpful Resources:

- **EPA Cybersecurity Procurement Evaluation Checklist:** The Cybersecurity Procurement Evaluation Checklist helps water and wastewater utilities assess the cybersecurity practices of vendors, manufacturers, and service providers. It includes a checklist specifically for Integrators and Managed Service Providers (MSPs) designed for companies that manage and deliver IT services and products to utilities.
- **CISA's Supply Chain Risk Management (SCRM) Essentials**: The SCRM Essentials guide provides a structured approach for organizations to identify, assess, and manage risks across their supply chain. It outlines key steps such as mapping suppliers, verifying vendor security practices, and continuously evaluating supply chain risks to strengthen organizational resilience.
- **WaterISAC's 12 Cybersecurity Fundamentals for Water and Wastewater Utilities**: Fundamental 11, "Secure the Supply Chain (service providers, integrators, and other "trusted" third parties)," provides guidance for managing vendor risk by enforcing security requirements, limiting third-party access, and maintaining strong oversight of external relationships.

Additional Reading:

- **CISA – Defending Against Software Supply Chain Attacks**
- **NIST – Key Practices in Cyber Supply Chain Risk Management**
- **Microsoft Security Blog – Supply Chain Attacks**
- **Trend Micro – Defending Software Supply Chains Against Attacks**

ASK THE EXPERT: Interview with DC Water's Director of Security

Water and wastewater utilities face a complex and evolving physical threat landscape. Security personnel must balance the need for strong physical security measures with the operational demands of maintaining reliable, uninterrupted water and wastewater services. As cyber-physical convergence continues to grow across utility systems, security teams face increasing pressure to protect interconnected operational technologies without hindering efficiency, system performance, or critical maintenance activities.

To help understand these challenges and learn methods to enhance a utility's physical security posture, we spoke with Ivelisse Cassas, Director of Security at DC Water, in Washington, D.C., to offer her perspective on physical security best practices for the water and wastewater sector to help utilities drive down risk.

Q: What are the most critical physical threats facing water utilities today, and how have those threats evolved over the past few years?

A: From a physical security perspective, water utilities continue to face risks like unauthorized access, theft and vandalism—especially at remote or lightly staffed facilities—but the threat has evolved beyond traditional perimeter concerns. While cyber threats are rightly top of mind across the sector, I think it's critical to recognize insider threat as a growing physical security issue.

Insiders already have legitimate access, operational knowledge, and familiarity with systems and facilities, which means they can bypass controls in ways external actors cannot. Many cyber and operational incidents are still enabled by physical access to sensitive areas like treatment processes, control rooms, or network closets—even in environments that aren't internetconnected. As utilities expand remote operations, contractor access, and thirdparty partnerships, the focus must shift from just keeping people out to actively managing and monitoring who already has access—and how that access is used.

Q: What are the most common security gaps you see across water utilities, and how can organizations realistically address them?

A: I could list several common security gaps across water utilities, but I want to focus on the one area that every organization can easily get their arms around and actually do something about: keys and lock management. Over time, physical access tends to sprawl—keys aren't always tracked or returned, locks aren't rekeyed, and access expands without regular review. That creates real risk, particularly when those keys open critical spaces like treatment areas, control rooms, or network closets. Addressing this doesn't require new technology or major investment; it starts with governance—knowing what keys exist, who has them, why they have them, and routinely validating that access. Once utilities get this right, it becomes much easier to tackle other gaps like contractor access, remote facility security, and overall insider threat risk.

DC Water's Blue Plains Advanced Wastewater Treatment Plant

Q: How do you balance physical security and operational efficiency, especially with limited resources?

A: I don't think of physical security and operational efficiency as something you have to trade off—they work best when they're integrated. My approach starts with partnership and listening: understanding how the work actually gets done and where the real operational pressures are. With limited resources, we stay focused on what truly matters and apply security in a way that supports the mission rather than slowing it down. When security expectations are clear and built into daily operations, they reduce friction instead of creating it.

A good example is how we approach things like camera placement. Rather than installing security measures in isolation, we work with operations to understand workflows, safety concerns, and how spaces are used day to day. That collaboration helps ensure cameras and controls are placed where they add real value—supporting accountability, safety, and awareness—without interfering with how people do their jobs. When security is designed with operations instead of around them, it strengthens both efficiency and risk reduction.

Continues on page 4

Q: How do you train and engage non-security staff—such as operators and maintenance crews—to be part of the security posture?

A: I don't approach this as training nonsecurity staff so much as engaging them as partners in the security posture. Operators and maintenance crews already understand the facilities, systems, and risks better than anyone—they just don't always label those things as security. We focus on regular conversations instead of onetime training: explaining the *why* behind controls, listening to concerns, and tying security expectations back to reliability, safety, and accountability.

Just as important is being accessible and communicative. Operations run 24/7—and so does security. Our teams know they can reach the Security Command Center via call or email at any time for support, questions, or to report concerns. I also make myself personally available—by phone, text, or email—because responsiveness builds trust, even if that means being reachable at all hours with a very short window for sleep. But I'm always reinforcing: use the security group email and Security Command Center. That ensures nothing gets missed and that the right support is in place, even if I'm not the first call. When people know Security is there to support them, not police them, they're more engaged, more aware, and far more willing to speak up when something doesn't look right.

Q: Relatedly, how important is security awareness training, and how can utilities conduct in-house training?

A: We all know security awareness is important, but how it's delivered matters just as much as the message itself. We focus on keeping awareness practical and approachable rather than formal or overcomplicated. Much of our training is done inhouse using simple tools—short videos recorded on an iPhone and edited with basic Microsoft Clip software—to show real security expectations in real operational spaces. We also incorporate scenariobased training around topics like deescalation, responding *until help arrives*, and activethreat awareness. We reinforce these concepts through brief, periodic messages and by attending foremen allhands meetings to listen, answer questions, and connect security back to daytoday work. That mix of simple tools, realworld scenarios, and facetoface engagement builds awareness and shared responsibility without pulling people away from operations.

Q: Can you walk us through a real incident (or near miss) and what changes you implemented afterward?

A: In 2020, at the height of COVID, we experienced a serious workplaceviolence incident at one of our heavily populated locations that I describe as an activethreat near miss. The incident stemmed from a verbal altercation between an employee and a supervisor. The individual was asked to leave the workplace, which they did; they were placed on administrative leave in coordination with Labor Relations; and Security was immediately notified (by the supervisor and Labor Relations), a step made possible by strong working relationships and clear escalation protocols.

Although access was denied at a primary entrance, the individual later gained entry through an unmanned access point with the unintended assistance of another employee who was unaware the individual was not authorized to be on site. This highlighted how uncertainty and fear can influence splitsecond decisions and expose gaps in access governance. Shortly afterward, shots were fired on the property, and the incident tragically resulted in a selfinflicted fatality. Law enforcement responded quickly, and there were no additional injuries or impacts to operations.

This incident reshaped how we approach workplace violence, insider risk, and access control. It reinforced that threats don't always present externally, that behavioral indicators often appear first, and that access governance is only effective when people understand their role. As a result, we strengthened coordination with Labor Relations, addressed unmanned access points, tightened access controls, and expanded scenariobased training focused on deescalation, *untilhelparrives* actions, and activethreat awareness. The key lesson was clear: layered security only works when communication, policy, access, and workforce awareness are aligned.

Q: What partnerships (such as local law enforcement, federal agencies, or industry groups) have been most valuable, and how should utilities approach building those relationships?

A: Partnerships are essential—utilities can't manage today's threat environment alone. At the local and regional level, our relationships with DC Homeland Security and Emergency Management Agency (HSEMA), the Metropolitan Police Department, and the regional fusion center have been especially valuable for realtime information sharing, coordinated response, and situational awareness. Federally and at the sector level, WaterISAC, the FBI, and CISA play a critical role in helping us understand emerging physical and cyber threats, learn from peer utilities, and stay aligned with national risk priorities.

For utilities looking to build these relationships, the recommendation is simple: engage early and often. Connect with your local fusion center, participate in exercises and briefings, leverage WaterISAC resources, and establish relationships with law enforcement and CISA before there's an incident. Partnerships are most effective when they're operational, trusted, and sustained—so when something happens, coordination is already in place and response isn't starting from scratch.

Iranian Cyber Threat to U.S. Water and Wastewater Utilities Amid the Conflict with Iran

Amid ongoing hostilities between the U.S. and Iran, the cybersecurity threat to U.S. water and wastewater utilities from Iranian threat actors is significantly elevated. On April 7, the FBI, CISA, EPA and other federal partners issued a joint Cybersecurity Advisory (CSA) titled "**Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across U.S. Critical Infrastructure**." The authoring agencies urgently warned U.S. organizations of ongoing cyber exploitation of internet-connected OT devices, including **Rockwell Automation/Allen-Bradley**-manufactured programmable logic controllers (PLCs) (and likely others), across multiple critical infrastructure sectors.

Since the release of the advisory, EPA and WaterISAC have observed continued targeting of PLCs and other industrial control system (ICS) devices by Iranian threat actors.

The CSA indicates that multiple U.S. critical infrastructure organizations across sectors (particularly Government Services and Facilities, including local municipalities; Water and Wastewater; and Energy) experienced disruptions through malicious interactions with project files and the manipulation of data displayed on HMI and SCADA displays. In a few cases, this activity has resulted in operational disruption and financial loss.

WaterISAC and EPA urge utility operators to review the joint CSA, including the tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) for indications of current and historical activity on their networks, and apply the recommendations listed in the mitigations section to reduce the risk of compromise.

Additionally, Censys released a report on April 7 that identifies 5,219 internet-exposed Rockwell/Allen-Bradley PLCs globally (3,891 in the U.S.). The report details co-exposed services and a list of IOCs that can be used in conjunction with **CISA's recently published IOC list**.

Recently, attention has turned toward the newly discovered **ZionSiphon** malware, which contains targeting logic centered around water treatment and desalination environments. Despite the fanfare, Dragos released a **blog post** that maintains ZionSiphon is not a credible threat, describing it as a poor attempt at generating OT malware using a large language model (LLM) and calling the attention the malware has generated "hype." Regardless, even if the malware itself is not currently assessed as credible, its development reflects a clear intent by threat actors to create tools capable of disrupting water systems and warrants close observation and awareness by defenders.

In addition to OT-focused activity, Iranian advanced persistent threat (APT) operations continue to target enterprise environments through evolving social engineering techniques. For example, **CyberProof reports** that the Seedworm APT has leveraged Microsoft Teams-based impersonation of IT support personnel to deliver malware and establish persistent access, demonstrating continued innovation in initial access vectors and blending of legitimate tools with malicious activity. Taken together, these developments reinforce that Iranian cyber operations remain active, adaptive, and positioned to escalate quickly.

Other recent cyber developments highlight the ongoing challenges facing the water sector. In March 2026, for example, a significant ransomware attack impacted the Minot Water Treatment Plant Minot in North Dakota, rendering the SCADA system inoperable and forcing operators to revert to manual gauge readings for 16 hours during restoration.

Additionally, the emergence of Anthropic Mythos in April 2026 marks a generational shift in cybersecurity, as it is the first AI model capable of autonomously discovering and exploiting zero-day vulnerabilities on an industrial scale. While Anthropic has restricted its release to protect critical infrastructure sectors, the model's capabilities present a unique and severe threat to the Water and Wastewater sector and other OT environments.

Open-source reporting suggests the current U.S.–Iran ceasefire is **unlikely to deter retaliatory cyber activity**. *Handala*, the Iranian-backed threat group responsible for the incident at Stryker, posted on social media saying: "let it be clear: The cyber war did not begin with the military, and it will not end with any military ceasefire." Cybersecurity experts assess the warning should be taken seriously regardless of the ceasefire and, therefore, network defenders should maintain heightened vigilance for malicious cyber activity targeting the water sector.

***Read the full advisory here*.**

Additional Reading:

- **Iran Threat Overview and Advisories**
- **Iranian Cyber Threat Evolution: From MBR Wipers to Identity Weaponization**
- **Iranian Cyber Operations Enter Critical Window as Kinetic Conflict Reaches Day 94**
- **MedTech Giant Stryker Crippled by Iran-Linked Hacker Attack**

Iran Physical Security Threats and Supply Chain Disruptions Stemming from the Conflict

Today, the Iranian regime and its terrorist and criminal proxies continue to present a dynamic multi-domain threat to the United States and its allies, both overseas and in their homelands. The threat of targeted physical attacks in the U.S. homeland stemming from the U.S.-Iran conflict is a concern.

The Islamic Republic of Iran is the world's foremost state sponsor of terrorism. Acting through the Islamic Revolutionary Guard Corps (IRGC), Iran actively funds, trains, and provides operational support to multiple terrorist/militant groups in the Middle East, who serve its national interest and are termed the "Axis of Resistance." The threat to the West from Iran-linked threat actors is significant and multifaceted, operating through four simultaneous vectors: Iranian agents (IRGC and Ministry of Intelligence and Security), Iran-funded or -supported terrorist organizations acting independently or as proxies (Hezbollah and Hamas), criminal proxies (e.g., Mexican drug cartels and Hells Angels), and radicalized lone offenders.

In recent years, Iran and its proxies have targeted critical infrastructure and planned attacks against U.S.-based military facilities. Specifically, over the past five years, U.S. authorities have disrupted **at least seventeen Iranian-linked plots** in the homeland involving regime operatives and/or terrorist and criminal proxies.

The potential threats to the U.S. homeland and critical infrastructure remain similar to what was described in DHS's **National Terrorism Advisory System (NTAS) Bulletin**, which was issued following the U.S. strikes on Iran's nuclear facilities in July 2025. The bulletin stated that "the ongoing Israel-Iran conflict could contribute to US-based individuals plotting additional attacks." The NTAS bulletin stated that conflict could "motivate violent extremists and hate crime perpetrators seeking to attack targets perceived to be Jewish, pro-Israel, or linked to the US government or military in the Homeland."

Accordingly, the most likely threat would be from U.S.-based homegrown violent extremists (HVEs) who are motivated by foreign terrorist organizations or Islamic Revolutionary Guard Corps (IRGC) operatives. Notably, on March 1, two top Iranian religious leaders issued separate fatwas calling on Muslims worldwide to take revenge for the killing of the Iranian Supreme Leader.

HVEs are often motivated by flashpoints, including geopolitical events, and may quickly mobilize to violence using simple tactics and readily available weapons. For instance, the attacker who conducted a mass **shooting** at a bar in Austin, Texas, on March 1,

was motivated by the U.S. conflict with Iran.

In addition, U.S. officials remain **concerned** about the potential risk from Iranian "sleeper cells." For example, the IRGC-QF publicly **warned** that "the enemy should know that their happy days are over and they will no longer be safe anywhere in the world, not even in their own homes."

The threat of Iran hiring criminal proxies to conduct attacks in the homeland is also a real concern, and one that federal authorities successfully thwarted, according to the Department of Justice. On May 15, U.S. officials **arrested** and charged a key leader within the Iraq-based, Iran-backed militia Kataib Hezbollah (KH), following his role in planning at least 20 attacks on American, Canadian, and European soil.

The individual was reportedly the central coordinator behind the Iranian-linked front group Harakat Ashab al-Yamin al-Islamiyya (HAYI), which claimed responsibility for at least 18 attacks in Europe since the start of the conflict. These attacks included bombings, arson, and assaults targeting American communities and interests. More recently, the terrorist leader plotted to attack local communities in New York, California, and Arizona. Ultimately, as the conflict between the U.S. and Iran continues, the potential for targeted violence in the U.S. remains elevated.

Supply Chain risks

Supply chain impacts due to the disruption in maritime shipping is another consequence of the ongoing conflict. Energy prices due to the disruption are elevated causing inflation to rise and other cascading impacts.

Seaborne sulfur shipments have suffered a significant decline, leading to rising **prices** and fears of

shrinking **supply**. Sulfur is not used directly in water treatment. However, it is a primary component in the production of sulfuric acid and sulfur-based chemicals, including sulfur dioxide, according to the **EPA**. Sulfur is also a key input for many different industrial processes, such as copper mining.

In March, WaterISAC and EPA received information from sector partners that an Israeli supplier of hydrofluorosilicic acid (HFS), a phosphate fertilizer byproduct which is used in the water sector for drinking water fluoridation, announced its intention to exit the U.S. market due to workforce shortages. The supplier, ICL, has lost a large part of its workforce due to individuals being called into active military service. ICL's announcement led one HFS distributor, Coyne Chemical, to declare a force majeure. Two utilities also reported that their HFS supplies had been impacted because of this disruption.

Relatedly, there is a potential for increasing costs of plastics, which might affect the cost and availability of plastic products (such as plastic piping) used by many utilities. Helium, which is vital for artificial intelligence chip production, and fertilizers, key to global food security, are also facing supply chain disruptions. Meanwhile, aluminum prices are approaching their highest level in four years, following smelter closures caused by conflict in the Gulf region, which supplies about 10% of the world's aluminum.

Additional Reading:

- **The Iran War and the Global Terrorism Threat**
- **Violence-as-a-Service: Iran's Digital Recruitment Model and the Homeland Threat**
- **U.S. Arrest of Kataib Hezbollah Leader Signals a Shift in Iranian Proxy Model**
- **Between Intent and Capability: Assessing the Lack of Iranian Attacks on the U.S. Homeland**
- **Gulf chemicals supply disruption will continue for months to years**

The 2026 National Cybersecurity Drill, "A Day Without SCADA," on July 8 at 1:00 PM ET

Training and exercises are critical for helping water and wastewater utilities build, improve, and validate their plans, policies, and procedures while strengthening their operational resilience and ensuring their security practices are appropriate for today's complex threat landscape.

Hosted by EPA, this discussion-based and operations-oriented exercise challenges water and wastewater utilities to maintain critical services during a simulated, multi-region telecommunications and internet outage. Utilities can participate by either practicing manual operations at their facility or joining a tabletop exercise session.

Key goals include:

- Testing operational survival without digital connectivity.
- Evaluating response plans and manual workarounds.
- Uncovering preparedness gaps and resource needs.

This drill strengthens sector resilience, helps identify critical dependencies, and ensures the continued delivery of safe and clean water under severely degraded conditions.

Register for the drill here.

EPA has a comprehensive website to help utilities design and conduct tabletop exercises (TTX). The TTX tool section provides users with the resources to plan, conduct and evaluate tabletop exercises. It offers multiple threat scenarios stemming from hazards across the all-hazards threat environment, such as cyber attacks, flooding, earthquakes, acts of vandalism, and more. ***Access EPA's TTX tool page here***.

EPA also offers general resilience training, such as its All-hazards Boot Camp Training, which is a self-paced training course that provides an overview of how water and wastewater systems can build resilience to all-hazards. In addition, utilities can access topic specific resilience training and review guidance documents on developing your own training courses. ***Access EPA's resilience training here***.

INSIDER THREAT CORNER – Third-Party Risk

Third-party vendor insider threats are a critical vulnerability for the water and wastewater sector. These threats arise when trusted, authorized third parties, such as maintenance contractors, software providers, system integrators, and administrative companies, misuse their access, either maliciously or unintentionally. Water facilities can also be affected indirectly through insider threats when third-party vendors endure cyber-attacks and other breaches. Examples of third-party insider threats are listed below:

- Janitorial staff can pose a significant insider threat risk because they have physical access to facilities, control rooms, and in some cases, insecurely placed computers or network jacks, creating opportunities for both accidental and malicious harm. This vulnerability significantly increases when the janitorial staff work after hours and regular staff are not present, leaving them in the facility without supervision or escort.
- A large drinking water utility experienced a hazmat incident at its treatment plant as a result of an unintentional insider error from a third-party vendor. The vendor mistakenly offloaded a chemical into the wrong tank, which raised alarm about a possible hazmat situation. An evacuation order was issued for many hours as firefighters and first responders evaluated the situation and took appropriate actions to render the area safe.
- A small drinking water utility hired a financial firm to handle administrative tasks such as collecting payments, maintaining financial records, depositing money and providing financial reports to the utility. According to a civil lawsuit, the mother/son small company allegedly created false financial statements, wrote unauthorized checks, and stole more than $680,000 from the utility company.

Water utilities can mitigate the risk of third-party insider threats by implementing a layered insider threat program that combines physical security,

access management, personnel oversight, and continuous monitoring. Consistent with guidance from CISA, utilities should apply the principles of least privilege and need-to-know access for contractors, vendors, and other third parties, ensuring individuals only have access to the systems, facilities, and operational areas required for their specific work.

Utilities should also conduct background screenings, require cybersecurity and security awareness training, monitor contractor activity in sensitive areas, and regularly review physical and digital access permissions to prevent unnecessary or lingering access. Because insider threats involve individuals with authorized access and operational knowledge, utilities should establish cross-functional reporting and monitoring processes that help identify concerning behaviors, unusual access patterns, or policy violations before they escalate into operational disruptions or security incidents.

Additional Reading:

- CISA - Insider Threat Mitigation Guide
- Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective
- Third-Party Risk Management – Evaluating Cyber Risk Posed by IT and Managed Service Providers

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)