INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

Water and Wastewater Critical Infrastructure

Institute for Homeland Security

Sam Houston State University

Robert Warren

CONTENTS

ABSTRACT

Water and wastewater utilities represent a pivotal element within the network of critical infrastructure sectors. Their interconnectivity with other sectors underscores the importance of security and protection measures. This paper delineates the regulatory and operational challenges water and wastewater utility operators face, highlighting the complex landscape of critical infrastructure security. It delves into the distinct concerns related to water and wastewater utilities and how these issues compound the difficulty of safeguarding such essential services. Amid growing threats to the United States critical infrastructure, especially domestic and foreign terrorism, this study underscores the imperative measures required to bolster the security and resilience of water and wastewater systems.

Critical Infrastructure Security
The foundation of critical infrastructure security, particularly for the water and wastewater sector, is deeply intertwined with national security, economic stability, and public health. Drawing on the National Infrastructure Protection Plan (NIPP) and Presidential Policy Directive PPD-21, this paper expounds on security as a multifaceted approach to mitigating risks through physical and cyber defensive measures. It stresses the importance of comprehensive strategies in threat and vulnerability management. It highlights the role of information sharing and cooperative efforts across various government and private sector levels. The Texas Homeland Security Strategic Plan is an example of state-level initiatives designed to enhance security and promote resilience in the face of potential incidents.

Water and Wastewater Sector
The critical role of water and wastewater services in public health, environmental protection, and economic activity cannot be overstated. With significant portions of the U.S. population relying on public drinking water and wastewater treatment systems, the vulnerability of these services to attacks—ranging from contamination and physical damage to cyber threats—poses severe risks. This section explores the potential consequences of such vulnerabilities, including public health crises and disruptions to essential services. Emphasizing the necessity of stringent security measures, the paper advocates for enhanced protective actions to secure the water and wastewater sector against various natural and man-made threats.

CRITICAL INFRASTRUCTURE SECURITY

First, it is necessary to understand critical infrastructure security and the role water and wastewater play in communities to establish the needs for the water and wastewater critical infrastructure sector.

According to the National Infrastructure Protection Plan (NIPP), critical infrastructure represents systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The National Plan acknowledges that the nation's critical infrastructure is primarily owned and operated by the private sector; however, federal, state, local, tribal, and territorial governments also own and operate critical infrastructure, as do foreign entities and companies. *(National Infrastructure Protection Plan, 2013)*

Presidential Policy Directive PPD-21 Critical Infrastructure Security and Resilience defines security as reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. Securing critical infrastructure systems includes several elements, including addressing threats and vulnerabilities, sharing accurate information, and analyzing current and future risks. Prevention and protection activities contribute to strengthening critical infrastructure security. *(Presidential Policy Directive PPD-21, Critical Infrastructure Security and Resilience, 2013)*

From a practical perspective, security encompasses multiple layers of protection intended to deter, detect, deny, delay, and defend against various threats and vulnerabilities to an organization's people, property, and information.

The Texas Homeland Security Strategic Plan addresses securing Texas and enhancing its resilience to incidents that do occur, which requires close coordination among jurisdictions at all levels. This strategy applies to state and local agencies, and Texas also encourages and recognizes the critical importance of voluntary private-sector cooperation. Effective implementation of the state's homeland security strategic plan requires active monitoring, assessment, and management of homeland security risk and corresponding adjustments to our priorities and activities. *(Texas Homeland Security Strategic Plan, 2021)*

Water and Wastewater Sector

Safe drinking water protects public health and supports all human activities. Properly treating wastewater is crucial for preventing disease and safeguarding the environment. Therefore, ensuring the provision of clean drinking water, as well as proper wastewater treatment and services, is vital for modern life and the nation's economy. There are approximately 153,000 public drinking water systems and more than 16,000 publicly owned wastewater treatment systems in the United States. More than 80 percent of the U.S. population receives potable water from these drinking water systems, and about 75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems (*Water and Wastewater Systems, Cyber and Infrastructure Security Agency, 2015)*.

The Water and Wastewater Systems Sector is vulnerable to various attacks, including contamination of finished water, contamination of source water, physical attacks, theft of resources, diversion impacting operations, sabotage, and cyberattacks. The result of various attacks could be large numbers of illnesses or casualties and a denial of service that would also affect public health and economic vitality. The water and wastewater sector is vulnerable to natural disasters. Critical services such as firefighting,

correctional facilities, healthcare (hospitals), and other dependent and interdependent sectors, such as Energy, Food and Agriculture, and Transportation Systems, would suffer degradation or negative consequences from a lack of service within a few hours. The following table shows the impact of degradation on critical infrastructure sectors due to a lack of service by the water and wastewater sector:

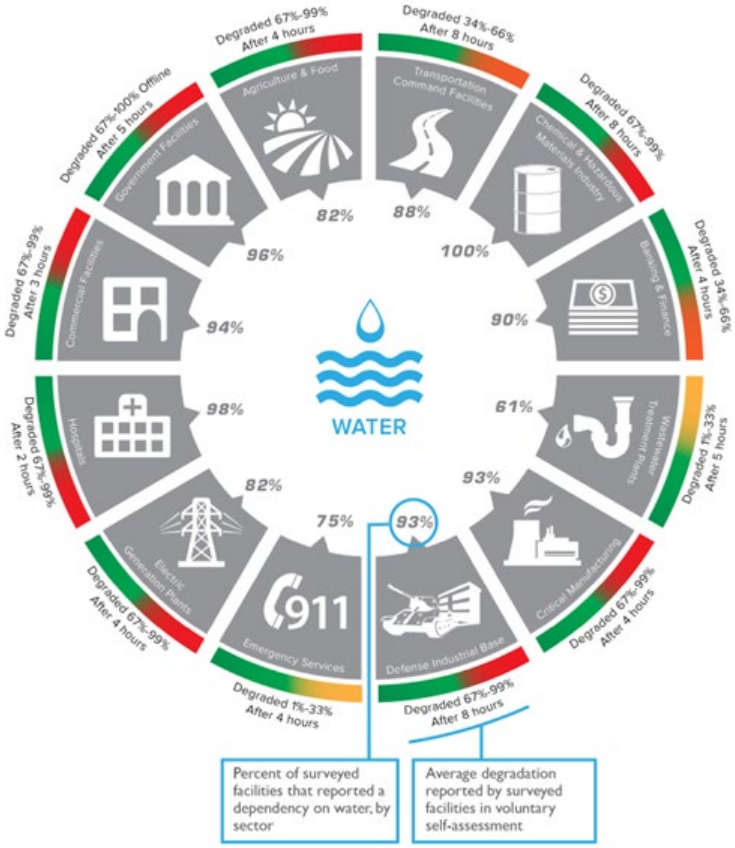

Figure 1. Impact of loss of water service on critical infrastructure sectors, Source CISA

Additionally, the ability to supply water and manage wastewater are considered National Critical Functions—which are functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

The term sector-specific agency means a federal department or agency designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in all hazards environment in coordination with the Department. For example, water and wastewater sectors may have the following Sector-Specific Agency that is tasked with critical infrastructure security and resilience:

- The Environmental Protection Agency (EPA) is designated as the Sector Risk Management Agency for the Water and Wastewater Systems Sector (Primary).
- Department of Homeland Security – dams, government facilities, transportation.
- Department of Energy – Power generation as it relates to water (Hydroelectric, Biogas power generation).

On October 23, 2018, America's Water Infrastructure Act (AWIA) was signed into law. The AWIA section 2013, which amended section 1433 of the Safe Drinking Water Act (SDWA), requires community drinking water systems serving more than 3,300 people to develop or update risk and resilience assessments (RRAs) and emergency response plans (ERPs). RRAs evaluate the vulnerabilities, threats, and consequences of potential hazards. The SDWA section 1433 requires that RRAs shall assess the risks to and resilience of specified assets to malevolent acts and natural hazards, including:

- Physical barriers.
- Source water.
- Pipes and constructed conveyances, water collection, and intake.
- Pretreatment and treatment.
- Storage and distribution facilities.
- Electronic, computer, or other automated systems (including the security of such systems).
- Monitoring practices.
- Financial infrastructure.
- The use, storage, or handling of chemicals.
- Operation and maintenance of the system.

The EPA does not specify the format in which utility owners must complete the RRAs, but formats are available to help with their completion. Most formats include physical and cybersecurity assessment elements and should involve the utility's security staff in conducting these assessments.

From a physical security standpoint, utility owners may consider using the RCAP (Rural Community Assistance Partnership) Security Vulnerability Self-Assessment Guide, designed to help small water systems determine possible vulnerable components and identify security measures that should be considered. The American Water Works Association (AWWA) also published the J100-21 Risk and Resilience Management of Water and Wastewater Systems, which includes a methodology for conducting a Risk and Resilience Assessment for a water utility.

The Texas Commission on Environmental Quality (TCEQ) has regulatory authority over several federal and state-identified critical infrastructures and essential resources, including water supply systems, wastewater treatment plants, chemical plants, low-level radioactive waste, refineries, and dams. TCEQ standards and regulations that govern the operations of water and wastewater utilities are strictly enforced, including specific requirements for physical security and access control.

Additionally, many public water systems rely on reservoirs to provide source water to produce drinking water, which may include those with hydroelectric power generation as part of its operations. Dams with hydroelectric power generation are subject to security regulatory oversight by the Federal Energy Regulatory Commission (FERC) Division of Dam Safety and Inspections. Dam Safety Inspections provide a chance to examine and evaluate the in-place security measures and to monitor and comment on their effectiveness against the current threat conditions or perceived by the licensee, typically the owner and operator of the dam/reservoir. In addition, this guidance provides a nationally consistent framework in which FERC dam owners can design and implement their security programs.

According to the Texas Homeland Security Strategic Plan, protecting critical infrastructure, including water and wastewater facilities in Texas, is a crucial element of the state's plan. Water and Wastewater Sector in Texas is represented as follows:

- Groundwater in Texas comes from 31 aquifers.
- The nine major aquifers supply about 90% of the groundwater used by Texans.
- Approximately 75% of all groundwater in Texas is used for crop irrigation.
- Texas has over 4600 community public water systems, which serve at least 15 residential service connections or 25 residents year-round.
- There are over 50 desalination plants in Texas.
- El Paso has the largest inland desalination plant in the world, with a production capacity of approximately 27.5 million gallons of potable water a day.
- There are 2513 active permits for public and private domestic wastewater treatment facilities in Texas.

WATER / WASTEWATER UTILITY ADMINISTRATION – SECURITY CONSIDERATIONS

The administration of a security program by a water or wastewater utility owner/operator can look different depending on the utility's size; however, some elements should be considered. Industry consensus standards guide administering security operations to align with best practices. Effective security management is the balance between regulatory compliance and industry best practices.

Many industry-specific associations and organizations support the professional standards and development of utility operations and their professionals. One of the largest is the American Water Works Association (AWWA). AWWA creates consensus standards related to water and wastewater utility programs. The AWWA G430-14 Security Practices for Operation and Management standard was developed to define the minimum requirements for a protective security program for a water, wastewater, or reuse utility that will promote the protection of employee safety, public health, public safety, and public confidence. This standard can be an excellent resource for evaluating water and wastewater utility security practices. Additionally, various committees are associated with the water and wastewater professional associations, emphasizing security and critical infrastructure protection and resilience.

Security Risk Management Considerations – Risk Management is a fundamental principle of security. In fact, in the recently released National Security Memorandum, NSM-22 Critical Infrastructure Security and Resilience, one of the policy principles and objectives is to consider a risk-based approach to protecting the nation's critical infrastructure. But what is risk and risk management? For many, risk may have a variety of definitions. From an enterprise risk management perspective, risk is the effect of uncertainty on positive or negative objectives. The Insurance Services Office (ISO) 31000 Enterprise Risk Management standard provides a framework for integrated risk-based decision-making regarding an organization’s governance, planning, management, reporting, policies, values, and culture. The Federal Emergency Management Agency (FEMA) defines risk as the product of three variables: threat, vulnerability, and consequence, and usually only focuses on the adverse risks. Enterprise Security Risk Management (ESRM) takes enterprise risk management principles. It applies a holistic security-specific focus to how security influences risk decision-making, defines the security professional's role, and helps establish a programmatic focus on administering security. ASIS International has provided professional standards for security professionals and many ESRM resources. Understanding how risk management impacts an organization can influence the effectiveness of a security program on a water and wastewater utility. Risk identification and risk analysis are the first steps of the risk management process an organization needs to take to address its security risks. Risk assessments can help determine the security risks impacting a critical infrastructure water and wastewater utility, identify strengths, opportunities, weaknesses, and threats, and help prioritize an organization's efforts and resources.

An outside perspective of the overall program administration and identifying risks for water and wastewater facilities is a best practice. The Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) operates the Protective Security Advisor (PSA) Program. PSAs are risk and resiliency subject matter experts who engage with Federal, State, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the nation’s critical infrastructure. The CISA PSA programs are offered to utility owners at no cost through a federal program. Water and wastewater essential infrastructure facilities are a priority focus for the CISA PSA program. The most widely used CISA PSA program is the Security Assessment at First Entry

(SAFE) assessment, a stand-alone assessment featuring standard language, high-level vulnerabilities, and options for consideration. SAFE is a rapid physical security assessment that assists facility owners and operators in implementing effective security programs. Using the SAFE assessment, CISA PSAs provide a structured review of a facility's security measures and deliver feedback on observed vulnerabilities and options for improving security. CISA includes water and wastewater utility management with a detailed report and risk score based on the findings of their assessments, along with recommendations and resources on how best to address those options for consideration.

For water and wastewater utilities to effectively carry out the functions of a physical security program, individuals need to be assigned to oversee program elements. Larger utilities may employ dedicated security personnel to staff and manage security positions. The qualifications of employees in a security role and their expertise in the physical security profession need to be considered. While law enforcement and emergency management have a significant role in security incident response, candidates in these roles typically do not emphasize physical or industrial security management. In general, the responsibilities of security management are to protect a utility's assets, not to enforce the laws of the public. However, a utility's security plan should include a strong working relationship with local enforcement to address response and security incident handling from a criminal standpoint. The local emergency management offices or local emergency planning committees are great resources for water and wastewater utilities and should have points of contact established. Candidates with a background in industrial security, security operations, system design or engineering, asset protection, or corporate security typically have a stronger foundation to lead security efforts for a utility. Specific professional designations further enhance the quality of security management positions, such as the certified protection professional (CPP) issued by ASIS International. The certified protection professional certification is designed for senior-level security managers with five to seven years of related experience, with at least three years in responsible charge of a security function (ASIS International, 2024). Having security management personnel with industry-accepted credentials provides legitimacy to a program that those individuals align with industry best practices. The continual professional development focused on protecting critical infrastructure, emerging trends, and technologies, as well as networking with peer organizations, enhance the profession of water and wastewater utility security management personnel. Many water and wastewater industry associations have committees and educational tracts to address security issues related to water and wastewater operations. Institutions for higher education also have professional development and certification programs emphasizing security and critical infrastructure to educate further and develop security professions.

When a water or wastewater utility is considering staffing security guard positions, ensuring individuals are licensed and in good standing to provide for this role is vital. Utilities outsourcing guard forces to third-party security firms can be an effective model for most water and wastewater facilities. Consideration should be given to firms with expertise in critical infrastructure protection and business models supporting the environment necessary to provide security for water and wastewater facilities. Larger firms can provide additional services such as off-site security operations monitoring and security consulting and typically have various forms of technology that can be leveraged to enhance a security program for a utility.

Clearly defined post orders are essential to any security guard post position that provides security for a water and wastewater facility. The post orders should be developed with the water and wastewater

utility owner/operator and the security guard service firm collectively and clearly outline expectations for the role, including daily activities, visitor management, security incident reporting, and more. Any deviation from established post orders is a breakdown in facility security and should be carefully monitored by security supervision.

Equally important to the professional security personnel are the non-security roles. Employees can be some of the greatest assets and threats to an organization's security. Having trained and vetted employees from a security standpoint can be a strong layer of protection to a facility's security profile. However, having employees who are complacent or uneducated on security procedures and threats can create danger by allowing a breakdown in security, impacting the facility or the water and wastewater utility as a whole. Criminal history background checks can be a principal element in managing the security risks to a water and wastewater utility. In most states, water and wastewater operators, maintenance personnel, engineers, security guards, and other technical roles must obtain and maintain an applicable license to be eligible for those roles, which would include some form of criminal history check as part of the licensing process.

Contractor management is another consideration for security management in a utility. Examples include chemical, supply, material, equipment deliveries, construction, maintenance contractors, and professional engineering and architectural providers supporting water and wastewater operations. Utility owners can start during the contracting process to address security concerns for items such as contractor background checks, providing lists of subs, clearly defined scope of service, and frequency of access to utility facilities. Managing site access through approved vendor lists, credential verification, and vehicle signage and identification helps a water and wastewater utility owner and operator track who has permissible access to their facilities. Contractors should be restricted to areas needed to do their work and escorted to security and safety-sensitive areas to prevent issues. Vendors accessing networks and security systems warrant further background checks, tighter restrictions, and additional requirements to protect the integrity of these systems. Collecting the credentials of discontinued contractors is a best practice to prevent unauthorized access attempts.

A vital element of a security program is a process for reporting, investigating, and tracking security incidents when they occur. A matter of best practice is to train and empower employees to identify security issues and report them to management for investigation and reporting. An effective security program includes a system for collecting security reports to track and trend incidents as they occur. Documentation of reported security issues helps identify trends useful for decision-making when prioritizing security resources. By including local law enforcement in security activities, reporting creates awareness for the local authorities and aids in criminal investigations if warranted. Many regulations require specific reporting criteria and timelines as well as methods for reporting. Utility owners and operators must have these requirements defined in their operating procedures or plans and security post-orders for security guards.

Security Information And Intelligence Sharing

Security information and intelligence are critical components impacting security operations for any organization, including water and wastewater utilities. Information gathered by utilities and local, state, and federal agencies creates opportunities for collaboration and timely sharing of information related to threats impacting various sectors and regions. Information and intelligence require intentional effort to protect the process of information sharing while at the same time promoting secure lines of

communication across industry lines. Various organizations specialize in the administration of security information and intelligence sharing.

Federal, state, and local agencies rely on the fusion center model to administer the systematic information-sharing process. The Homeland Security Information Network (HSIN) is the Department of Homeland Security's official system for trusted sharing of Sensitive but Unclassified (SBU) information between federal, state, local, territorial, tribal, international, and private sector partners. Mission operators use HSIN to access Homeland Security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe. Certain utility security professionals may qualify for elevated security clearance to access federal security briefings related to credible threats to their sector.

The Texas Department of Public Safety Intelligence and Counterterrorism (ICT) division provides Integrated Statewide Public Safety Intelligence through a multi-jurisdictional public safety intelligence network. This network can generate tactical, operational, and strategic intelligence that supports public safety practitioners and policymakers. ICT operates the Texas Fusion Center in collaboration with federal and local law enforcement and fusion centers and administers the Texas Suspicious Activity Reporting Network. Utility security professionals can participate in the Infrastructure Liaison Officer (ILO) program to connect with the state's fusion center and receive regular intelligence updates. *(Texas Department of Public Safety Intelligence & Counterterrorism, 2024)*

InfraGard is a public-private partnership between the Federal Bureau of Investigation (FBI) and private sector members to protect U.S. Critical Infrastructure. InfraGard connects owners and operators within critical infrastructure to the FBI through seamless collaboration to provide education, information sharing, networking, and workshops on emerging technologies and threats. InfraGard's membership includes business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT (Informational Technology) professionals, academia, and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security. *(InfraGard, 2024)*

Open-source intelligence (OSINT) is the practice of gathering, analyzing, and disseminating information from publicly available sources to address specific intelligence requirements. Of all the threat intelligence subtypes, open-source intelligence (OSINT) is the most widely used, which makes sense. While OSINT is an excellent resource for security professionals, it also is one of the greatest threats to the security of a utility. Examples of OSINT include social media, Google Earth/Maps, search engines, and now the ever-growing artificial intelligence.

Another security information consideration for public utility owners and operators is related to the federal Freedom of Information Act (FIOA) or Texas Public Information Act (PIA), which are statutes intended to support public trust for publicly funded entities and utilities. However, open records create security concerns for information related to security-sensitive critical infrastructure information. Many states, including Texas, also have regulations dictating how long public records are maintained, accessed, and disposed of. Public utilities must balance public trust and public safety and security by managing information and documents related to the transaction of business and information about public utilities. Certain physical security elements are protected from open records requests, and others may be approved on a case-by-case basis by the attorney general after making a written request for consideration. Examples of security elements that may be withheld include specific details, blueprints,

or plans that outline the physical security components of a facility that, if known, would threaten public utility security.

Like the public information and government records statutes, public utilities may be subject to open meetings statutes that are transparent and open and provide opportunities for public participation in the official business of a public utility. From a security perspective, open meetings create open-source information security risk and personal security due to physical access to government officials. Utilities need to consider the security of these meetings while allowing for public access and participation. The design and structure of meetings and facilities to limit access to publicly accessible portions of the facility while encouraging public participation requires planning and execution.

Security System Technology, Regulations, And Design Guidelines

The use of technology in the market has improved the effectiveness and efficiency of physical security and critical infrastructure, allowing utility owners to create a more advanced security environment. Technology enhances a utility's security posture, often replacing or reducing the need for physical resources such as guard force, physical barriers, and manual processes, thus improving the efficiency and cost-effectiveness of security systems. Common security systems for water and wastewater utilities include security cameras and video management systems, access control, visitor management, and emergency communications. Technological advancements have enhanced the process of securing facilities in a connected environment. Enterprise security applications provide greater visibility and integration, along with data and analytics, to support security administration for critical infrastructure utilities. However, these advances have also resulted in new vulnerabilities that bad actors can exploit to compromise the security of critical infrastructure facilities. In response to these vulnerabilities, state and federal governments have prevented terrorist groups from exploiting vulnerabilities in connected technology, particularly in communications equipment and components associated with critical infrastructure protection systems.

- Section 889 of the John S. McCain National Defense Authorization Act (NDAA) prohibits the purchase of covered telecommunications equipment and services by government agencies from vendors selling spyware products. These devices could pose a threat to U.S. security by spying on or disrupting communications within the U.S. *(Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment, 2020)*

- In Texas, the Lone Star Infrastructure Protection Act of 2021 prohibits Texas businesses and governments from contracting with entities owned or controlled by individuals from China, Russia, North Korea, and Iran if the contracting relates to critical infrastructure and provides the foreign party with remote access or control of the necessary infrastructure. *(TX Govt Code § 2275.0102, 2023).*

Despite regulations, many utility owners and operators are overwhelmed with security technology options that offer inexpensive access to critical systems, such as video, access control, and emergency communications. They may be using products that do not comply with these requirements, inadvertently exposing their water and wastewater systems to businesses influenced by nation-states intending to spy on or disrupt US critical infrastructure. Security professionals must collaborate closely with utility owners and operators to ensure that only technology approved as NDAA compliant can be

used for security video, access control, emergency communications equipment, or connected to any network device on the utility's enterprise or industrial networks. Resources are available to assist utility owners and security professionals design and evaluate security systems:

- Water and Wastewater Security System Design Guidelines – EPA's standards and best practices for consideration. The EPA has established resources that guide enhancing security monitoring at utility facilities in a distribution system at risk of intentional contamination.

The use of small unmanned aircraft systems (UAS) or drones has been an increasing concern for critical infrastructure. While UAS/drones may be used to conduct day-to-day business operations and for the joy of recreational opportunities, misuse of these aircraft can pose significant challenges to America's critical infrastructure. These threats include:

- Weaponizing or Smuggling Payloads.
- Prohibited Surveillance and Reconnaissance.
- Intellectual Property Theft.
- Intentional Disruption or Harassment.

As a result of these threats, state and federal regulations prohibit UAS/drone use in proximity to critical infrastructure facilities. According to the Federal Aviation Administration (FAA), UAS/drones are prohibited from flying over designated national security-sensitive facilities. Operations are not permitted from the ground up to 400 feet above ground level and apply to all types and purposes of UAS flight operations and certain critical infrastructures. Texas Government Code 423.0045 prohibits the operation of unmanned aircraft within 400 feet of critical infrastructure facilities, including but not limited to water intake structures, water treatment facilities, wastewater treatment plants, pump stations, and dams that are classified as a high hazard by the Texas Commission on Environmental Quality, which all may be components of a water or wastewater utility in the state.

Enforcement of these regulations can be challenging, but collaboration with federal and local authorities is recommended. Criminal charges can be brought against those violating regulations, and additional restrictions, such as Temporary Flight Restrictions (TFR), may be imposed. Anti-drone technology is an emerging resource that utility owners and operators may employ. Signage, communication, and written drone procedures are effective administrative tools to address drone operations around critical infrastructure water and wastewater facilities.

To help assist critical infrastructure owners and operators address these security concerns, additional resources include:

- Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) UAS Fact Sheet.
- Cybersecurity Guidance: Chinese-Manufactured UAS.
- Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems.
- Secure Your Drone: Privacy and Data Protection Guidance.
- Department of Defense (DoD) – Defense Innovation Unit (DIU) Approves Fourteen sUAS/Drones Manufacturers (Updated December 2023).
- Federal Aviation Administration (FAA) Resources.
- B4UFLY Mobil App.
- No Drone Sign Template.

PHYSICAL SECURITY DESIGN CRITERIA

How water and wastewater infrastructure facilities are designed can significantly affect the overall security posture. Often, bad actors look for unprotected or vulnerable soft targets, or those with little to no security protection, to focus their efforts. Water and wastewater utilities must define what design standards and criteria will be incorporated in facility design, construction, and ongoing maintenance.

The process of detecting, delaying, deterring, denying, or defending against bad actors from focusing their intentions against a facility by stronger security layers. These include visible facility hardening, use of security systems, and physical presence of security features such as walls, fences, lighting, cameras, doors and windows, signage, shrubbery, etc., significantly reducing the likelihood of a security breach. This is known as hardening from a security standpoint. Having a good understanding of what critical assets impact the operations of a water or wastewater utility can help prioritize resources and focus design efforts from a protection standpoint. Certain industry design standards guide owners and operators of water and wastewater utilities for the best practices and elements of a secure facility. Figure 2 below represents the Concentric Circles of physical protection.

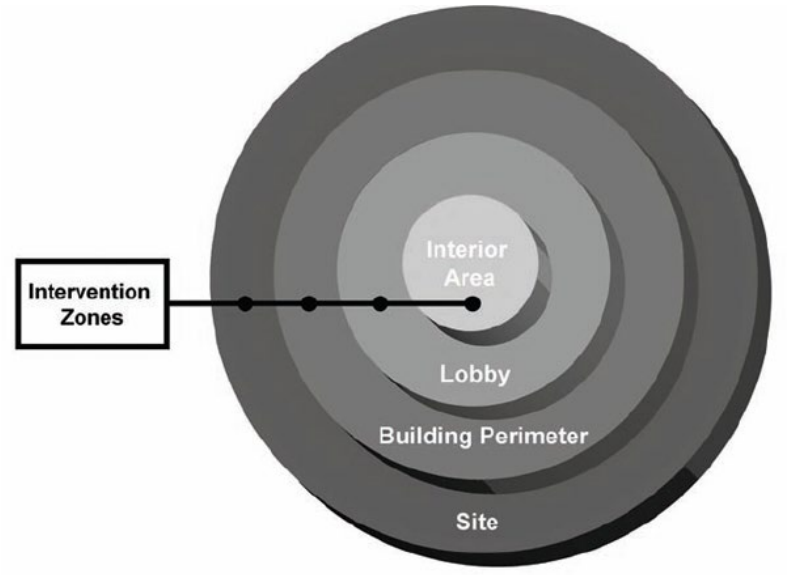

Figure 2. Concentric Circles of Physical Security

Crime Prevention Through Environmental Design (CPTED) is a multi-disciplinary approach to crime prevention that uses urban and architectural design and the management of built and natural environments. Pronounced as 'sep-ted,' CPTED is often referenced in many standards and guidelines to assist with considering components that impact a facility's security. CPTED strategies aim to reduce victimization, deter offender decisions that precede criminal acts, and build a sense of community among inhabitants so they can gain territorial control of areas, reduce crime, and minimize fear of crime. CPTED is otherwise known as Designing Out Crime, defensible space, and other similar terms. *(Security and Resilience - Protective Security - Guidelines for Crime Prevention Through Environmental Design, 2021)*

Water-and wastewater-specific design criteria often focus only on targeting the codes and standards to design and construct facilities for operability. However, considering the vulnerabilities and threats that water and wastewater facilities pose, security, safety, and resilience should also be considered. While

there may not be a sole source of reference for design criteria for these elements, some states, including Texas, have minimum design criteria that may include facility access, security, safety, and related requirements within the state's regulations with the intent to protect these critical infrastructure facilities.

Specific attention should be given to the type of hardware and construction methods used to secure water and wastewater facilities. From gate and door locking hardware to fencing material and construction, these physical elements, if appropriately designed, can provide a systematic approach to physical security. Examples include fail-secure locking hardware as permitted by local fire codes, redundant power supply for electronically controlled access points, using the most appropriate ANSI (American National Standards Institute) grade door and locking hardware for the application, key control and accountability, to name a few are all elements of an excellent physical security program from a design standpoint. Using a system for keys and locks, such as the Best System for systematic structuring of locks and locksets across an organization, helps with refined key and lock control and accountability while creating checks and balances and systematically administrating these hardware elements. Additionally, proper preventative and corrective maintenance of doors, gates, key locks, and other physical security is crucial to the overall success of these security elements.

The American Society of Civil Engineers published the Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities, ASCE/EWRI 78-24, which provides guidelines on the evaluation and enhancement of physical security of facilities used in potable water sources, treatment, and distribution systems, as well as for wastewater and stormwater facilities. This guidance document provides a comprehensive approach to integrating modern security practices into the management, operation, construction, or retrofit of water, wastewater, and stormwater systems.

CHEMICAL SECURITY

One of the most significant security threats that make water and wastewater infrastructure targets are the chemicals used to treat water and wastewater and the industrial equipment and processes at these facilities. Chemicals are a security concern for utility owners and operators. Examples could include theft or diversion of hazardous chemicals, intentional tampering with levels of chemicals impacting the safety of water within a facility or transmission line, or damage or vandalism to process control facilities or containers in an attempt to cause a dangerous release. Below are several program areas that address chemical safety and security impacting water and wastewater:

- Environmental Protection Agency (EPA) Risk Management Plan - The Risk Management Program (RMP) rule is implemented under Section 112(r) of the 1990 Clean Air Act amendments to improve chemical accident prevention at facilities. It requires facilities that use highly hazardous substances. Part of the requirements is to develop a Risk Management Plan that identifies the potential effects of a chemical accident, identifies steps the facility is taking to prevent an accident, and spells out emergency response procedures should an accident occur. Section 112(r)(1) of the Clean Air Act, also known as the General Duty Clause (GDC), makes the owners/operators of facilities with regulated hazardous substances responsible for managing chemicals safely. Many water and wastewater utilities, based on the types of chemicals used in the treatment process, fall under the EPA Risk Management Plan program requirements. *(Risk and Resilience Assessment and Emergency Response Plan Requirements, US Environmental Protection Agency, 2024)*

- Chemicals of Interest - Before July 28, 2023, the US Department of Homeland Security regulated certain chemicals through the Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 CFR Part 27). Appendix A lists more than 300 chemicals of interest (COI) and their respective screening threshold quantities (STQ) and concentrations. This program is under the Cybersecurity and Infrastructure Security Agency (CISA) oversight in a non-regulatory function. CISA's ChemLock program is entirely voluntary, providing facilities that possess dangerous chemicals with no-cost services and tools to help you better understand the risks you face and improve your chemical security posture in a way that works for your business model. Keeping hazardous chemicals out of the hands of those who misuse them is a responsibility shared between facility owners, operators, employees, emergency responders, and CISA. These COIs are categorized under three main security issues:

    - Release: Toxic, flammable, or explosive chemicals or materials that can be released at a facility.
    - Theft or Diversion: Chemicals or materials that, if stolen or diverted, can be converted into weapons using simple chemistry, equipment, or techniques.
    - Sabotage: Chemicals or materials that can be mixed with readily available materials.

    While water and wastewater utilities were exempted from the CFATS regulations, identifying chemicals of Interest (COI) and coordinating with CISA is a best practice. The first step to identifying chemicals of interest is to read Appendix A CFATS Chemicals of Interest (COI) list and compare this list to those a facility possesses or plans to possess any chemical(s). Any COI that meets or exceeds certain quantities and concentrations should be reported to CISA. Common chemicals of concern at water and wastewater facilities may include chlorine, sulfur dioxide, ammonia, hydrogen peroxide, flammable gases and substances, and lab chemicals and

substances. CISA has many resources to address chemical security, conduct on-site assessments, and provide assistance with training and exercise. (ChemLock, 2024)

- Transportation Security Administration (TSA) - Any utility that is designated as a rail hazardous materials receiver and is within a high-threat urban area, which means an area comprising one or more cities and surrounding areas, including a 10-mile buffer zone, as listed in 49 CFR Part 1580 Appendix A *(Freight Rail Transportation Security, 2020)*.

- Tier II—Hazardous Chemicals/Materials—Submission of the Tier II form is required under Section 312 of the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA). This form provides state, tribal, and local officials and the public with specific information on potential hazards. This includes the location and amount of hazardous chemicals present at facilities during the previous calendar year. Some states, such as Texas, may have specific requirements for reporting and submitting the Tier II inventory form and the state reporting form or format.

- Hazcom—right-to-know standards - To ensure chemical safety in the workplace, workers must have access to and understand information about the chemicals' identities and hazards. Knowing the hazards associated with chemicals also ensures proper handling, storage, and disposal of hazardous materials. Work environments with good chemical hygiene plans are more likely to have increased security considerations addressed by these safeguards. *(OSHA, 2012)*

CYBER SECURITY

Cyber-attacks against public water systems are increasing. Implementing basic cyber hygiene practices can help your utility prevent, detect, respond to, and recover from cyber incidents. Supervisory Control and Data Acquisition (SCADA) systems control, monitor, and analyze water and wastewater industrial and process control devices. These systems are considered the operational technology for a water and wastewater system. They are considered critical systems, meaning a compromise or denial of service to these systems can have a catastrophic impact on a utility's operations and potentially cause severe effects on the communities these utilities serve. Many water and wastewater utilities dedicate significant resources to isolating and protecting these networks of systems. Good cyber hygiene is essential to protect the security of industrial control networks. Like SCADA systems, security systems are critical and warrant best practices to prevent unauthorized activity or system failure. Examples of good cyber hygiene include:

- Strong password requirements and not sharing passwords.
- Maintaining system security updates and patches.
- Backup key systems and data frequently.
- Anti-virus software and firewall equipment to prevent and detect unauthorized activity.
- Separate critical systems from enterprise networks.
- Multi-factor authentication to access critical systems or networks.
- Training for all employees and individuals who access networks and systems.
- Contract language to address cyber controls and liability issues.
- Protecting sensitive data.
- Knowing how to identify and avoid social engineering and phishing activities.

A strong security program combines both physical and cyber security.

WAY FORWARD

Water and wastewater owners and operators must make intentional efforts to help ensure that the protection of this critical fracture aligns with ever-changing regulatory requirements and security industry best practices. As technology and threats evolve, utilities must adapt to stay proactive in their security operations.

REFERENCES

American Society of Civil Engineers, Guidelines for the Physical Security of Water and Wastewater/Stormwater Utilities, ASCE/EWRI 78-24, (2010) https://ascelibrary.org/doi/book/10.1061/9780784411261

America's Water Infrastructure Act of 2018, 33 USC 2201 (2018) https://www.congress.gov/bill/115th-congress/senate-bill/3021/text

American Water Works Association, AWWA G430-14 Security Practices for Operation and Management, (2014) https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/45322774

American Water Works Association AWWA J100-21 Risk and Resilience Management of Water and Wastewater Systems, (2021) https://engage.awwa.org/PersonifyEbusiness/Bookstore/Product-Details/productId/88116441

ASIS International, (2024) https://www.asisonline.org/

Baseline Information on Malevolent Acts for Community Water Systems 3.0, US Environmental Protection Agency, (2024) https://www.epa.gov/system/files/documents/2024-05/baseline_information_malevolent_acts_508_050724.pdf

Chemical Accident Provisions, 40 CFR Part 68 (1996) https://www.ecfr.gov/current/title-40/chapter-I/subchapter-C/part-68?toc=1

CISA, ChemLock, (2024) https://www.cisa.gov/resources-tools/programs/chemlock

CISA, Water and Wastewater Systems, (2024) https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector

Federal Aviation Administration (FAA) Unmanned Aircraft Systems (UAS) Critical Infrastructure and

Public Venues, (2023) https://www.faa.gov/uas/critical_infrastructure

Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment, 85 CFR 42665 (2020) https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain

Freedom of Information Act, 5 U.S.C. § 552 (2016) https://www.foia.gov/

Freight Rail Transportation Security, 49 CFR Part 1580 (2020) https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-D/part-1580

Homeland Security Information Network https://www.dhs.gov/homeland-security-information-network-hsin

InfraGard, (2024) https://www.infragard.org/

International Standards Organization (ISO), (2021), ISO 22341:2021 - Security and Resilience - Protective Security - Guidelines for Crime Prevention Through Environmental Design, https://www.iso.org/obp/ui/#iso:std:iso:22341:ed-1:v1:en

International Standards Organization (ISO), (2018) Risk Management ISO 31000 https://www.iso.org/iso-31000-risk-management.html

Lone Star Infrastructure Protection Act of 2021, Texas Government Code § 2275.0102 (2023) https://statutes.capitol.texas.gov/Docs/GV/htm/GV.421.htm#421

National Academies of Sciences, Engineering, and Medicine, (2011) Prudent Practices in the Laboratory: Handling and Management of Chemical Hazards, Updated Version. Washington, DC: The National Academies Press. https://doi.org/10.17226/12654

US Department of Homeland Security, *National Infrastructure Protection Plan (NIPP)*, (2013) https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf

National Security Memorandum NSM-22 Critical Infrastructure Security and Resilience, (2024) https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

Hazard Communication Standard, Occupational Safety and Health Administration (OSHA), (2012), https://www.osha.gov/hazcom

Presidential Policy Directive PPD-21, Critical Infrastructure Security and Resilience, (2013) https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and

Public Information Act, Texas Government Code, Chapter 552, (2023) https://www.texasattorneygeneral.gov/open-government/members-public/overview-public-information-act

Resources to Design and Implement Physical Security Monitoring for Surveillance and Response Systems, US Environmental Protection Agency (2017) https://www.epa.gov/waterresilience/resources-design-and-implement-physical-security-monitoring-surveillance-and

Risk and Resilience Assessment and Emergency Response Plan Requirements, US Environmental Protection Agency (2024) https://www.epa.gov/waterresilience/fact-sheet-risk-and-resilience-assessment-and-emergency-response-plan-requirements

Security Vulnerability Self-Assessment Guide, Rural Community Assistance Corporation (RCAP), (2005), https://www.tceq.texas.gov/downloads/assistance/water/pdws/rcap-pws-security-vulnerability-assessment-guide.pdf

Texas Commission on Environmental Quality Homeland Security, (2024) https://www.tceq.texas.gov/response/security

Texas Department of Public Safety Intelligence & Counterterrorism, (2024) https://www.dps.texas.gov/section/intelligence-counterterrorism

Texas Homeland Security Strategic Plan, (2021), https://gov.texas.gov/uploads/files/press/HSSP_2021-2025.pdf

AUTHOR BIOGRAPHY

Robert Warren is the Senior Manager of the Trinity River Authority of Texas' Risk Management Division, with extensive experience in Risk Management. Before joining the Authority, he was the Risk Manager for the City of Arlington and the Texas Department of Criminal Justice (TDCJ). Included in his many responsibilities, Robert manages the Authority's risk management, safety and emergency management, property and casualty insurance and claims, drug and alcohol program, security operations, records administration, and facility maintenance and fleet programs. Robert has served as a member of various boards and committees and has presented or contributed to publications at the state and national level in his official capacity. Robert was named Risk Manager of the Year by Texas PRIMA in 2017 and was awarded the Chapter Service Award at the National PRIMA. Robert is a licensed risk manager through the Texas Department of Insurance and holds a Master's Degree from Columbia Southern University in Occupational Safety and Health and a Bachelor's degree from Sam Houston State University in Business Administration. Additionally, Robert holds the Certified Risk Manager (CRM), PSHRA-HR Senior Certified Professional (IMPA-SCP), and Infrastructure Liaison Officer (ILO) designation.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Warren, R. (2024). Water and wastewater critical infrastructure protection (Report No. IHS/CR-2024-1038). Sam Houston State University, Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/PE32X