# Threat Analysis for the Water and Wastewater Sector

## January – June 2017

**Published December 19, 2017**

### Non-Disclosure Notice

*This document contains information that may be shared only with personnel who have a valid need to know. The document may not be shared with the public or the media, and it should be stored, handled, and disposed of securely. For questions regarding the storage, handling, distribution or disposal of this document, please contact analyst@waterisac.org or consult the WaterISAC Terms & Conditions.*

This page intentionally left blank.

# Contents

This page intentionally left blank.

# Background

## About WaterISAC

The Water Information Sharing and Analysis Center (WaterISAC) is the designated communications and operations arm of the United States Water and Wastewater Sector. WaterISAC helps utilities in the U.S., Canada, and Australia measure and reduce risk, improve resiliency, prepare for physical and cyber threats, and recover from disasters.

WaterISAC Pro members have access to the world's largest and richest source of information and tools for strengthening water and wastewater utility security, preparedness, resilience, and emergency management.

WaterISAC also supports federal, state, and local government agencies involved in water resources, law enforcement, emergency response, intelligence, and public health to inform programs and initiatives to protect critical infrastructure and public health.

WaterISAC is a non-profit organization created in 2002 by utility managers and is governed by a board appointed by the national water and wastewater associations, research foundations, and state drinking water administrators.

To log in to WaterISAC's secure portal, go to www.waterisac.org.

## Scope

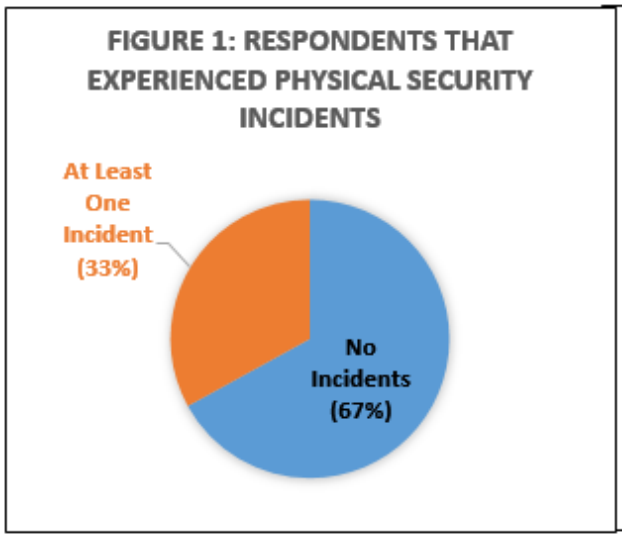
The Threat Analysis for the Water and Wastewater Sector examines incidents and suspicious activities at sector utilities between January 1 and June 30, 2017. The information on incidents and suspicious activities is derived from a variety of sources, including WaterISAC members who provided inputs via a survey and incident reports. A total of 120 organizations participated in a survey that contributed to this report; respondents were from 38 U.S. states and two Canadian provinces. The report also includes incident information from open sources and intelligence and analytical documents from federal, state, and local governments and law enforcement agencies, and other information sharing and analysis centers. The analysis in this document is solely the product of WaterISAC and does not necessarily reflect the views of other entities.

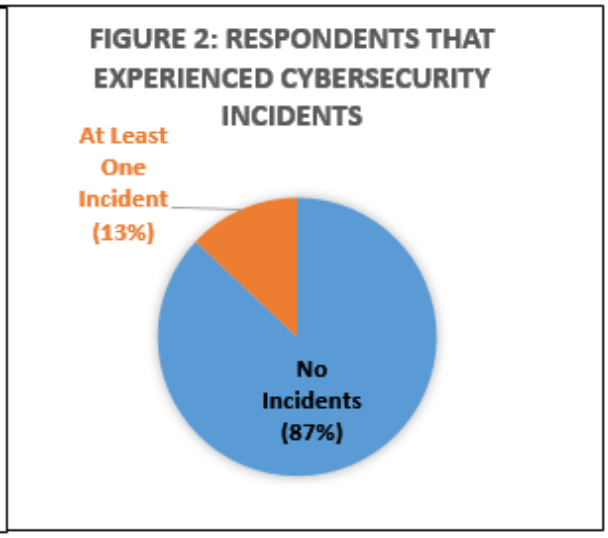
The events analyzed in this document should not be considered a comprehensive data set of all incidents and suspicious activities that occurred in the Water and Wastewater Sector. However, they do provide insights into the types of incidents occurring at sector assets.

This page intentionally left blank.

## Analysis of Sector Incidents

In the survey, utilities were asked to indicate whether they had experienced any physical or cyber incidents. Approximately 33% reported physical security incidents during the first half of 2017, a reduction from the second half of 2016 when 38% of respondents reported having experienced incidents. Approximately 13% of respondents reported at least one cybersecurity incident, up from the previous period's 9%.



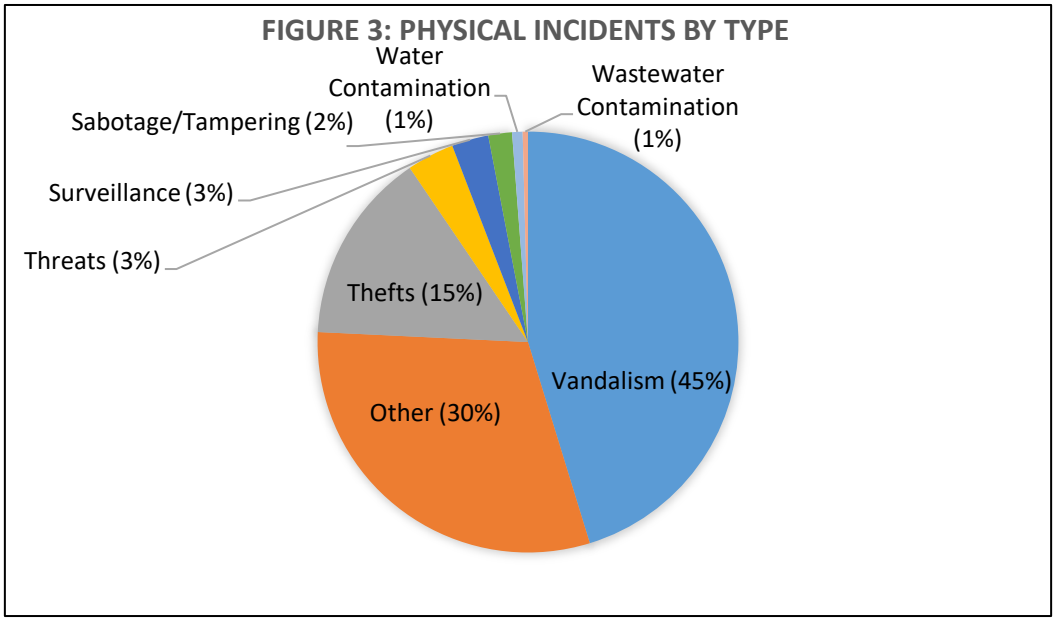



This page intentionally left blank.

## Physical Security Incidents

WaterISAC asked members to report the following types of physical security incidents, both completed and attempted: sabotage/tampering; contamination of water supplies; contamination of wastewater; surveillance; threats against facility or people (e.g., bomb threats and assault); theft of equipment, supplies, chemicals, or funds; vandalism and defaced or damaged property; and other physical security incidents. Definitions of each of the incident categories are included in the Appendix. Descriptions of notable incidents within each of these categories are captured below.

**FIGURE 3: PHYSICAL INCIDENTS BY TYPE**




### Vandalism (45%)

Graffiti was the most common type of vandalism during this period. Incidents of damage to chain-link fencing, security gates, or other measures protecting restricted areas were also reported in conjunction with defacement or theft attempts. The most notable incidents in this category included:

- One respondent reported that all the windows on a piece of equipment used by the utility were shot out.
- One respondent reported that a phone line distribution box next to a water tower had been vandalized.

### Other (30%)

This category captures traditionally less threatening or destructive offenses, such as trespassing, suspicious activity, and relatively minor violations of organizational policy. The most notable incidents involved:

- One facility experienced a communications outage after a fiber optic cable was severed by a gunshot during a domestic dispute in the neighborhood.
- An unknown male posed as an employee of a utility to obtain large amounts of a dechlorinating agent from a local vendor.
- Staff were disrupted by law enforcement activity happening adjacent to their facility, which included a fatality. This event necessitated participating in interviews with law enforcement authorities and crisis counseling.
- At one utility, there were multiple instances of non-authorized persons trespassing to hike, fish, or take a shortcut across its land.

The following incidents were reported to WaterISAC separately from the survey:

- A third-party water neutralizer supplier was contacted through email for the purchase of four boxes of ascorbic acid, four chlorine monitoring kits, and four boxes of calcium thiosulfate. The emailer was not knowledgeable about the products, would not state name or affiliation, and sent emails seven hours ahead of local time. The person also wanted the product shipped to a city in a different state.
- A water utility operator discovered an individual breaking into a water plant gate. The individual pulled a gun on the operator, who immediately left and called police. Police responded in 90 minutes. Gas chlorine cylinders were located on-site.
- An unknown subject breached security and trespassed onto a water treatment plant by first scaling the cyclone mesh perimeter fence then digging and crawling through a hole under the interior fence. The subject used tools to burglarize locked utility vehicles and enter a paint shop office. The person stole items, including small hand tools and keys to a vehicle. There was no breach to the water system. The police department was notified of the incident.
- A man driving a pickup truck attempted to gain access to restricted areas of a wastewater treatment plant to take photos of his vehicle in various locations. His request was denied.

### Theft of Equipment, Supplies, or Funds (15%)

Most thefts reported to WaterISAC were perpetrated by outsiders. One respondent reported a person stealing water from a fire hydrant. The following types of equipment and supplies were reported as having been stolen:

- Currency
- Materials made of copper and brass, including tools, wire, and scrap metals
- A Federal Aviation Administration (FAA) hazard light
- Vehicles
- A laptop
- Lawn care equipment
- A security camera
- A portable generator

The following incident was reported to WaterISAC separately from the survey:

- A utility district employee's backpack containing six water access keys was stolen out of a work vehicle. Four of the keys were marked with key codes. The incident was reported to local police.

### Threats against a Facility or People (3%)

The majority of threats reported by respondents entailed varying levels of violence in retribution for utilities shutting off customers' water. Field personnel and customer service representatives were the most common target of these threats, which often referenced gun violence. These additional threats were reported:

- A former employee threatened workplace violence against a facility.
- "Moneylenders" contacted the utility searching for a staff member.
- A non-authorized pesron jumped into a vehicle owned by a utility to escape pursuers armed with guns.

### Surveillance (3%)

The largest number of incidents were related to drones flying over or observing treatment plants, watersheds, rail yards, and other restricted areas. One respondent reported a drone crashed into an open-air reservoir. The following incidents were also reported:

- A delivery driver attempted to use another person's ID to enter the area.
- An unknown person used binoculars to monitor a water treatment plant.
- In multiple instances, people lied in attempts to gain access to facilities.

The following incidents were reported to WaterISAC separately from the survey:

- Wastewater plant operators spotted a large drone flying along the north perimeter of a plant at about 100 feet in elevation in an eastward zig-zag flight pattern. The craft circled southward over the solids building and swung back to the west in the direction of the disinfection facilities. At that point contact with the drone was lost. This incident was reported to the area fusion center and to the local TSA contact.
- A person was observed by a citizen taking pictures over a fence of a new sewage pump station from directly across the street. The citizen took some pictures of the person and questioned them about what they were doing. The person immediately ran into the woods. The citizen reported the incident to the police and then notified pump station personnel. The station itself was locked and fenced. The only chemical stored on-site was diesel fuel.

### Sabotage/Tampering (2%)

One respondent reported an incident of their water treatment facility being shot at by an unknown person. There were no casualties and local police were notified.

The following incident was reported to WaterISAC separately from the survey:

- A water utility noticed the locks for a gate protecting a water tank and a vent atop the tank were cut. The area was put under a "do not drink" advisory. No contamination was detected.

### Water Contamination (1%)

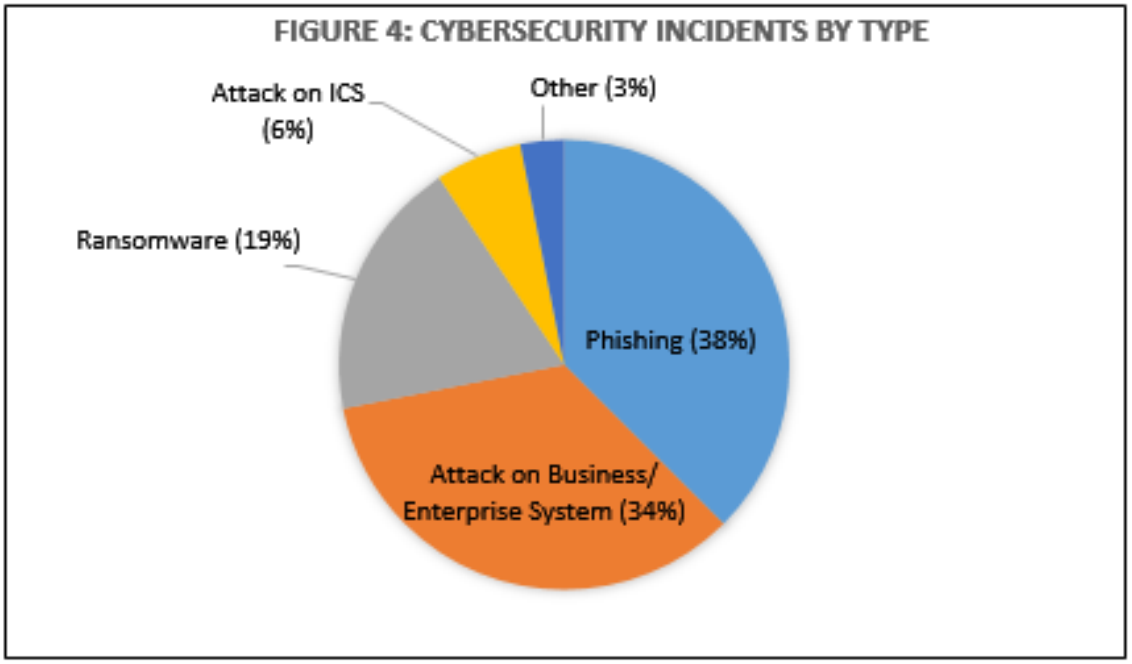
One respondent reported a contamination threat had been called in against their facility. No additional information was provided.

### Wastewater Contamination (1%)

One respondent reported their organization had experienced numerous cases of glycol reaching treatment plant. The respondent indicated the investigation is ongoing.

## Cybersecurity Incidents

WaterISAC asked members to report the following types of cybersecurity incidents, both successful and attempted: attacks against their industrial control system systems (ICS); attacks against their business/enterprise information systems; ransomware infections; phishing; and other. Definitions of each of the incident categories are included in Appendix C. Descriptions of notable incidents within each of these categories are captured below.




### Phishing (38%)

WaterISAC specifically asked members if any of the attacks involved phishing. Twelve respondents reported phishing attempts at their organizations. Some of the respondents elaborated on their experiences with phishing, which included:

- One respondent noted an employee's email account was compromised, which the perpetrator tried to leverage to obtain additional credentials.
- Two respondents noted incidents of CEO Fraud, a form of Business Email Compromise (BEC), as well as numerous other phishing attempts that had mostly been filtered out.
    - Wire Fraud – one respondent reported three spear phishing incidents of CEO Wire Fraud, in which a perpetrator pretends to be the CEO directing an urgent wire transfer.
    - W2 Fraud – one respondent reported an email sent to the human resources manager purporting to be the CEO asking for copies of all employee's W2 forms.

The email was quarantined, but the manager noticed and reported it. The respondent credits existing security measures and successful employee security training efforts for thwarting the attempt. Furthermore, this event was reported to the IRS Fraud Detection and Prevention Department.

- Four organizations reported having experienced regular phishing attempts, noting that none of these had been successful.
- One organization noted that employees receive numerous phishing emails but that none have resulted in a successful breach of the system.
- One respondent reported phishing attempts at their organization, a few of which were directed spear-phishing campaigns, but most of which were "spray and pray" types of attempts.
- WaterISAC received two possible phishing emails that were designed to appear as replies to WaterISAC's newsletter. They were sent from a forged local government employee email address that was not affiliated with a WaterISAC account. Each email included an attachment.

### Attack on Business/Enterprise System (34%)

A business/enterprise system entails an organization's information systems separate from its ICS/SCADA networks. Many of these attacks are perpetrated via malicious links embedded in emails or websites, or via unpatched vulnerabilities in software applications.

- Fifteen respondents reported attempted intrusions against their business/enterprise systems. Nine of the respondents confirmed several successful attempts, mostly due to phishing, ransomware, and other methods.
- One organization reported its website had been defaced by an Islamic State supporter.
- One respondent reported that their firewall was hacked as a cover to contact other servers. The same respondent also reported that some email accounts were hacked, but there was no resultant damage.
- An organization's website was compromised by a threat actor who had exploited an unknown vulnerability.

The following incident was reported to WaterISAC separately from the survey:

- A utility reported it had experienced collateral damage from a distributed denial of service (DDoS) attack on its Internet site host. The utility was not the intended victim, but access to its website was occasionally interrupted for a few days.

### Ransomware (19%)

WaterISAC specifically asked members if they had experienced a ransomware attack.

- One respondent noted the organization was the victim of successful ransomware infections on two servers.

- Three respondents reported their organizations detected ransomware (but the attacks don't seem to have been successful).
- Two organizations reported the attempts were not successful due to detection/protection capabilities.

### Attack on ICS (6%)

WaterISAC specifically asked members if they had experienced ICS attacks. Two organization acknowledged that they had, although no further details were provided.

### Other (3%)

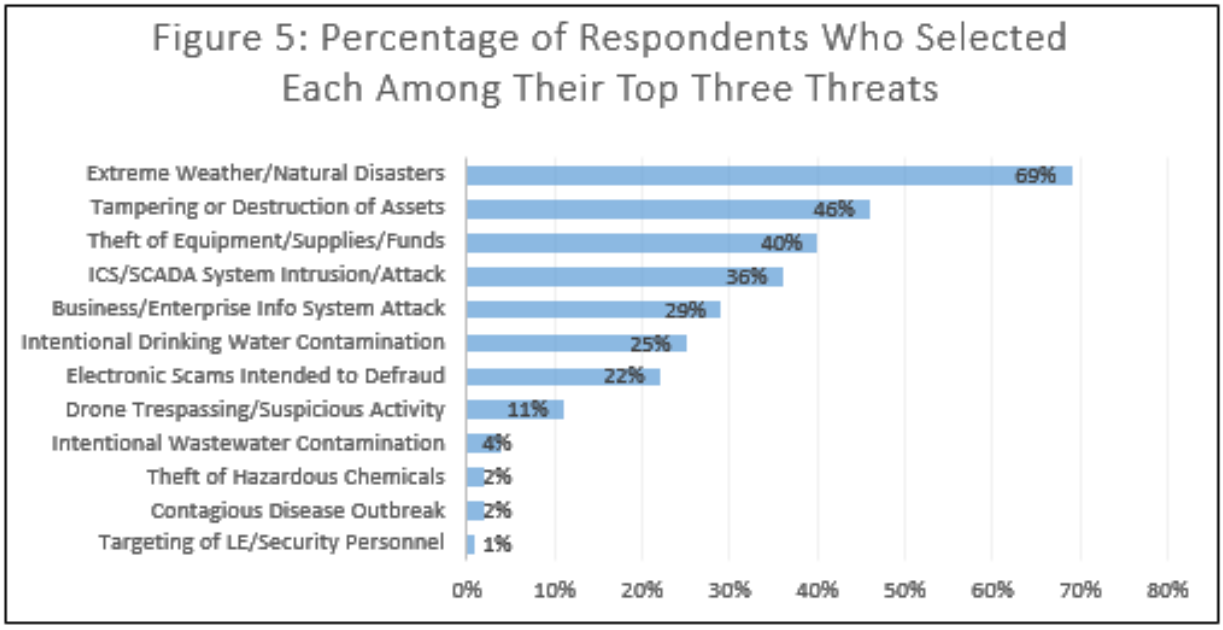
Other cyber-based attack methods not specifically categorized as phishing or ransomware.

- One organization reported a virus that infected its system is believed to have been introduced by a contractor connecting remotely to the network. The organization did not indicate if the infection affected its business enterprise system or its ICS.

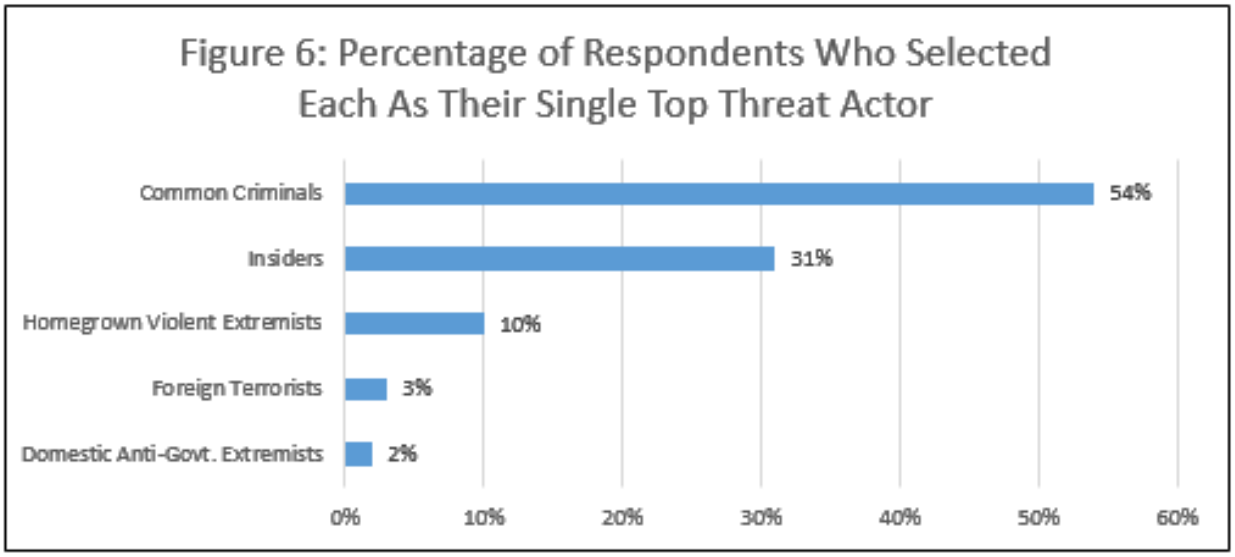
This page intentionally left blank

## Water and Wastewater Sector Threat Environment

The survey asked respondents to identify the cybersecurity and physical security threats they deemed to be most significant for the water and wastewater sector.




Additionally, the survey asked respondents to select the actors they believed represented the greatest threats to the sector.



This page intentionally left blank.

# Appendix A: Reporting Incidents and Suspicious Activities to WaterISAC

The threat environment described above reinforces the importance of continued awareness and vigilance. WaterISAC encourages all members to report any incidents, including crime and suspicious activities, regardless of scope or presumed credibility. Providing incident and suspicious activity information to WaterISAC allows analysts to evaluate trends in and threats to the water sector more accurately and to notify members of emerging threats in a timely manner.

Incidents can be reported to WaterISAC via any of the means identified below. WaterISAC recognizes the importance of confidentiality in reporting. Information identifying the reporting organization or individual is not disclosed to outside organizations without consent.

**Online Form** (accessible both on WaterISAC's secure portal and public website)
www.waterisac.org/incident

**Office Phone**
202-331-0479

**24-Hour Phone**
866-H2O-ISAC (866-426-4722)

**Analyst Email Address**
analyst@waterisac.org

**Physical and Mailing Address**
1620 I Street, NW, Suite 500
Washington, DC 20006

This page intentionally left blank.

# Appendix B: External Resources and Contact Information

**U.S. Centers for Disease Control and Prevention**
http://www.cdc.gov

**U.S. Department of Homeland Security (DHS)**
http://www.dhs.gov

**National Infrastructure Coordinating Center (NICC)**
To report incidents: Email: NICC@dhs.gov
Phone: 202-282-9201

**Protective Security Advisors (PSA)**
Please contact WaterISAC's Analyst Desk for PSA information

**United States Computer Emergency Readiness Team (US-CERT)**
https://www.us-cert.gov
To report incidents: Online Form: https://www.us-cert.gov/forms/report
Email: info@us-cert.gov
Phone: 888-282-0870

**Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**
https://ics-cert.us-cert.gov
To report incidents: Email: ics-cert@hq.dhs.gov
Phone: 877-776-7585

**U.S. Environmental Protection Agency (EPA)**
http://www.epa.gov
Water Security Division
https://www.epa.gov/waterresilience

**Federal Bureau of Investigation (FBI)**
https://www.fbi.gov
Field Offices
https://www.fbi.gov/contact-us/field/field-offices
Reporting Tips
https://tips.fbi.gov
Internet Crime Complaint Center (IC3)
https://www.ic3.gov

**Water and Wastewater Agency Response Networks (WARN)**
http://www.nationalwarn.org

# Appendix C: Types of Incidents and Suspicious Activities

**Contamination:** Unauthorized entry of an unwanted substance, such as a chemical or biological agent, into raw water supplies, treated drinking water, wastewater, or wastewater effluent.

**Cybersecurity Incident:** Compromising or attempting to compromise a facility's business/enterprise information systems or ICS/SCADA devices and infrastructure.

**Other Physical Security Incident:** This classification is intended to capture any physical security incidents that do not meet the criteria for the other categories. These incidents are typically less threatening or destructive. Trespassing, suspicious questioning or interactions with organization personnel, and relatively minor violations of organizational policy are examples of these types of incidents.

**Phishing:** The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

**Ransomware:** A type of malicious software that threatens to perpetually block access to a victim's data unless a ransom is paid.

**Sabotage / Tampering:** Deliberately damaging or manipulating part of a facility to obstruct, disrupt, or destroy operations.

**Surveillance:** Demonstrating unusual interest in a facility or its personnel and their activities. Surveillance can be conducted in person or remotely, such as through the use of binoculars or drones, and can involve the perpetrator making notes, drawing maps, or taking photographs.

**Theft:** Stealing organization equipment, supplies, chemicals, or funds.

**Threat of Malicious Action:** Stated intent to inflict pain, injury, damage or other hostile action on someone or something.

**Vandalism:** Criminal damage of property, including graffiti, defacement, or destruction. Unlike sabotage/tampering, acts of vandalism are primarily directed towards non-essential equipment and do not impact facility operations.