SURVEILLANCE AND SUSPICIOUS ACTIVITIES INDICATORS GUIDE

For Dams and Levees

July 2021

Cybersecurity and Infrastructure Security Agency

Table of Contents

Incident Response: Agency Contacts

List incident reporting or response agency contact information for your community and geographic region. Build relationships with these groups before an incident occurs.

Resource	Contact	Phone Number
City Law Enforcement		
County Law Enforcement		
State Law Enforcement		
Local Fire Service		
Department of Homeland Security (DHS) Protective Security Advisor		
DHS Cybersecurity Advisor		
CISA Central	www.us-cert.gov/report Central@cisa.dhs.gov	(202) 282-9201
Local Joint Terrorism Task Force		
Local Federal Bureau of Investigation (FBI) Office		
FBI Weapons of Mass Destruction Coordinator		
FBI Hotline		1-800-CALL-FBI (800-225-5324)
State Dam Safety Office		
Downstream Dam Operator		
Upstream Dam Operator		
City Emergency Management		
County Emergency Management		
State Emergency Management		
U.S. Coast Guard		
State Fusion Center		
Information Sharing and Analysis Center (ISAC) (e.g., WaterISAC, Electricity ISAC)	www.waterisac.org/report-incident www.eisac.com/login	866-H2O-ISAC (WaterISAC) (202) 790-6000 (E-ISAC)
Local Response Diving Unit		
Local Response Bomb Squad		

Acknowledgements

This document was developed with input, advice, and assistance from representatives from the public and private sector, including members of the Dams Sector Security Education Working Group, Levee Subsector Council, and the Dams Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC). For a complete list of GCC and SCC member organizations, visit www.cisa.gov/dams-sector-council-charters-and-membership.

The *Surveillance and Suspicious Activity Indicators Guide for Dams and Levees* provides dam and levee owners and operators with information on issues related to surveillance objectives, indicators of surveillance and suspicious activity, methods for reporting suspicious activity, and other actions to take to counter surveillance and suspicious activity. Originally published in 2017, this guide was updated in 2021 to provide additional information on reporting suspicious activity and to summarize actions that owners and operators can take to counter instances of surveillance and suspicious activity.

The cover photo, depicting The Dalles Dam in Oregon, is provided courtesy of the U.S. Department of Homeland Security (DHS).

Distribution

This *2021 Surveillance and Suspicious Activity Indicators Guide for Dams and Levees* was prepared under the auspices of the DHS Cybersecurity and Infrastructure Security Agency. For distribution information, contact the Dams Sector Management Team at DamsSector@cisa.dhs.gov.

Notice

Introduction

The Dams Sector includes a broad range of infrastructure facilities that provide hydroelectric power, river navigation, water supply, flood damage reduction, irrigation, waste management, and recreation. As with all critical infrastructure, Dams Sector assets may be the target of an attack that could result in severe economic losses, loss of life, and reduced public confidence in industry and the government's ability to provide essential services. To increase the probability of carrying out a successful attack, adversaries strive to avoid a target's strengths while focusing on the target's weaknesses. To accomplish these objectives, the attacker may conduct extensive planning, including surveillance. Many of the steps in the attack planning cycle can be discovered through observation and could result in suspicious activity reports (SAR) submitted by vigilant staff or protective measures implemented by facility personnel.

The *Surveillance and Suspicious Activity Indicators Guide for Dams and Levees* provides dam and levee owners and operators with information on issues related to surveillance objectives, indicators of surveillance and suspicious activity, methods for reporting suspicious activity, and other actions to take to counter surveillance and suspicious activity.

Surveillance is the systematic observation or monitoring of areas, places, persons, or things by visual, aural, electronic, photographic, or other means for the purpose of gathering intelligence otherwise unavailable or impractical to obtain. Suspicious activity is any observed behavior, including surveillance, that could indicate planning for a terrorist attack or other criminal activity. A wide variety of physical and cyber tactics and tools can be applied to conduct surveillance and collect data needed to carry out an attack. Suspicious activity that could be discovered include an adversary's actions to plan for an attack using explosives, weapons, or cyber means.

Owners and operators can take actions to increase employee awareness of suspicious activities, develop a culture of reporting suspicious activity, and implement security measures to counter instances of surveillance and other suspicious activity to disrupt the attack planning cycle. It is important for personnel to use careful observation skills, patience, and practice to discriminate between benign and provocative actions. Absent a specific, actionable threat, indicators of surveillance and suspicious activity should be used to aid security officials, law enforcement, and first responders in identifying and mitigating potential threats. Some behavioral indicators may be legal or constitutionally protected activities and should be supported by additional facts to justify increased suspicion. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any security response.

Attack Planning Cycle

To increase the probability of carrying out a successful attack, adversaries strive to avoid a target's strengths while focusing on the target's weaknesses. To accomplish these objectives, the attacker may conduct extensive planning, including several instances of surveillance. The attack planning cycle depicted in figure 1 identifies the critical steps that adversaries—such as terrorist organizations or other criminals—follow to plan and execute attacks on selected targets.

Figure 1. The Attack Planning Cycle

In the initial step in the attack cycle process, the attacker identifies and selects a target then plans a method of attack. Target and method selection are based on the likelihood of achieving the threat goals (e.g., cause injury or death, disrupt operations or the local economy, make a political statement, or enact vengeance on or embarrass the organization) and on the target's apparent criticality, vulnerabilities, and ability to respond. While selecting a target and attack method—proceeding through the planning cycle steps—the attacker conducts detailed surveillance of the area to assess security measures and identify physical barriers (e.g., fences, access restrictions) needing to be bypassed to access the intended target and successfully carry out the attack. Subsequent rounds of surveillance are used to determine if security measures changed, thus impacting the attack plan (e.g., new barriers placed, guards being posted at varying hours, K-9 patrols), and to ensure the target remains recognizable during all light and weather conditions. The adversary completes the cycle through final planning and rehearsals—to improve the odds of success, confirm planning assumptions, and develop contingencies—before proceeding to execution. Upon conclusion of the attack, adversaries may seek to escape or exploit the compromised facility or plan a fatal end. A prime objective of an operation is to exploit and publicize the attack.

The attack cycle depicted and described in this section is generally representative of an adversary's process. The number of steps and length of time from preliminary target selection to execution will vary depending on the complexity of the attack and the attacker's familiarity with the target. While the planning cycle may take years from inception to an attack, the planning cycle may occur in a matter of days to weeks. Globally, most terrorist attacks from the past decade have featured a faster process in which the attacker chose a familiar target and conducted minimal surveillance and/or pre-operational activity.

Many of the steps in the attack planning cycle can be discovered through observation and could result in SARs being submitted by vigilant staff or actions taken to increase the facility's security posture. For example, unauthorized persons attempting to approach restricted areas or asking unusual questions about technical matters could be an indicator of surveillance. Once discovered, an organization can submit a SAR with local authorities and/or alter or enhance their security measures to stop or mitigate the planning cycle. Subsequent chapters in this document expand on these concepts.

Surveillance

Surveillance is the systematic observation or monitoring of areas, places, persons, or things by visual, aural, electronic, photographic, or other means for the purpose of gathering intelligence otherwise unavailable or impractical to obtain. Indirect means may also be used to gather the information, such by recruiting employees (either voluntary or involuntary), eliciting information about the dam from employees or venders who have access to locations within or around the facility, or conducting Internet research on the facility. Surveillance is a key element in the attack planning cycle to determine possible targets, attack modes, and the likelihood of success of an attack against a critical infrastructure asset, while ideally remaining undetected. A wide variety of tactics and tools can be applied to conduct surveillance and collect data needed to carry out an attack.

Objectives of Critical Infrastructure Surveillance

Adversaries engage in surveillance activities to identify security vulnerabilities that can be exploited. To be effective in meeting this goal, the adversary must have a line of sight to the target's vulnerability, blend into the environment and remain undetected, and gain access and egress from the surveillance position with out drawing attention to themselves. After surveillance of a target has concluded and preparations for the attack are complete, a final pre-attack surveillance determines whether changes in surroundings or conditions will impact the adversary's ability to carry out a successful attack. Throughout this process, an adversary's specific surveillance objectives could be to identify any of the following features of an asset:

- Presence or absence of security cameras
- Number, location, type, and coverage of security cameras
- Identification cards of employees and contractors
- Security screening procedures for employees, visitors, and contractors
- Security event response times and type of response
- Access point locations or accessibility
- Opportunities for cascading damage effects
- Locations and characteristics of vulnerable structural components
- Areas of weakness observed during a flood event
- Intrusion opportunities such as broken locks, damaged fencing, or doors
- Patterns of concentration of people and vehicles
- Locations where further surveillance can take place

How Surveillance is Conducted

Progressive Surveillance

Adversaries may observe a target for a short time from one position, withdraw for a time (possibly days or even weeks), then resume surveillance from another position. This progressive surveillance activity may continue until the adversary determines that the asset is a suitable target. This type of transient action can make the surveillance more difficult to detect or predict but may also provide a greater chance for interdiction by dam or levee personnel and/or law enforcement. During this process, the adversary may utilize mobile or fixed surveillance methods:

- **Mobile surveillance** consists of observing the facility or site operations by driving, boating, or walking by a site or viewing the site via an unmanned aircraft system (UAS). With regards to levees, mobile surveillance would likely be conducted by driving or walking the length of a levee and looking for a suitable point of attack. This might be at a point where the levee is weakest or where the damage caused by its failure would be most severe. Indications of mobile surveillance activity include the repeated presence of an unfamiliar vehicle in the area, the presence of UAS near a critical asset, or persons walking on or around the levee for reasons that do not seem obvious.
- **Fixed surveillance** is a more typical tactic for targeting dam infrastructure because it is conducted from a static, often concealed position. Adversaries may establish themselves in a public location over an extended period of time, such as at a recreational area close to a dam, and utilize technology to capture the data needed to inform attack plans. They may also pose as a fisherman, tourist, delivery personnel, photographer, or demonstrator to provide a plausible reason for being in the area repeatedly or for an extended period of time.

Surveillance Technology

Modern technologies readily available to consumers have aided adversary efforts to view facility operations, security protocols, and personnel movements. Typical examples of optical and photographic devices used by adversaries to conduct surveillance include binoculars, telescopes, cameras, cell phones, and radio scanners. Advanced technologies include thermal imagers and satellite imagery to locate and possibly identify equipment and personnel not otherwise detected by other optical devices (i.e., during poor weather, behind visual barriers, inside buildings).

Unmanned Aircraft Systems

In addition to recreational use, UAS—also known as unmanned aerial vehicles or drones—are used throughout the Dams Sector to gain situational awareness by conducting remote patrols, conducting inspections, and monitoring operations. Despite legitimate uses, UAS is an increasing concern for multiple critical infrastructure sectors due to the relative ease of adversaries procuring some models that require relatively little skill to operate. Therefore, the amount of time spent on planning for the attack can be reduced. In the Dams Sector, the primary threat from UAS is surveillance of the facility, including identifying specific targets, security assets, or security protocols. In addition, a UAS carrying a weaponized payload may present a threat to associated structures and assets or large groups of people congregating at the facility.

Insider Threat

Insider threat arises when employees or contractors use their knowledge of the facility, its operations, and its vulnerabilities to conduct acts of sabotage or provide sensitive information or facility access to an outsider. Insiders that are complacent or simply unaware can prove equally as damaging to an organization. Sharing credentials (e.g., access card, computer passwords), falling for phishing scams, or holding open access-controlled doors are all examples of how an adversary may exploit an insider's access to gain knowledge about the facility and carry out an attack.

Cyber Incidents

Cybersecurity in the Dams Sector is primarily focused on the industrial control systems (ICS) that monitor, automate, and control critical physical processes, such as electric generation and transmission, water level and transport, and physical access control. A cyber event affecting ICS can allow attackers to remotely direct these physical processes and cause infrastructure damage, disrupt operations, or cause collateral damage to essential services and nearby communities. A cyber event

affecting information technology (IT) systems could compromise business operations or facilitate theft of sensitive business or customer information, potentially leading to operational compromises and/or significant economic losses. A skilled cyber threat actor can pivot from an IT enterprise network to an operational technology environment if controls are not fully implemented and monitored. Phishing scams, watering holes, and probing of cyber defenses are a few examples of strategies used by adversaries to infiltrate systems to conduct surveillance and launch cyber attacks. A number of cyber incidents affecting critical infrastructure likewise leverage compromised remote access technologies, including virtual private networks (VPNs) and remote desktop sharing.

Indicators of Possible Surveillance

Understanding the operational mindset and techniques of an adversary conducting surveillance can make it easier for facility personnel to spot the adversary. While there is no signature look of an adversary's surveillance, indicators are based on an adversary's actions or activities deemed unusual for the location in which they are taking place. Therefore, it is important for personnel to use careful observation skills, patience, and practice to discriminate between benign and provocative actions. The following list of surveillance activity indicators illustrates possible warning signs. Items marked with an asterisk (*) are also possible indicators of an insider threat and should be investigated and treated according to organizational procedure.

Absent a specific, actionable threat, indicators of surveillance should be used to aid security officials, law enforcement, and first responders in identifying and mitigating potential threats. Some behavioral indicators may be constitutionally protected activities and should be supported by additional facts to justify increased suspicion. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

Human Indicators (observed or reported):

- Persons using video, camera, or observation equipment and/or UAS to take pictures or videos of infrastructure or security measures in an unusual or surreptitious manner.
- Persons with facility maps, photos, or diagrams with highlighted areas or notes regarding infrastructure or a listing of facility personnel.
- Persons possessing or observed using night-vision devices near the levee or dam perimeter or in the local area with no apparent reasonable explanation.
- Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
- Nonmilitary persons seen with military-style weapons and clothing/equipment.
- Persons questioning personnel offsite (i.e., via personal email, telephone, fax, or postal mail) to elicit information about the dam or levee, including its critical features and/or security practices.
- Persons not associated with the dam or levee showing an increased general interest in the area surrounding it.
- Dam or levee personnel maintaining unofficial and regular contact with persons soliciting information about the levee or dam at a level beyond mere curiosity.*

- Persons attempting unauthorized access (i.e., criminal hacking) of computers, systems, or websites looking for personal information, maps, or other targeting examples.*
- An employee changing working behavior or working more irregular hours without approval or a reasonable explanation.*
- Persons observing deliveries, especially of hazardous or toxic materials.
- Aircraft or UAS flying in restricted airspace or a boat encroaching into restricted areas, especially if near a critical infrastructure asset.
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services.
- Theft of employee or contractor identification cards or uniforms, or unauthorized persons in possession of identification cards or uniforms.
- Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, security cameras, intrusion detection systems, electric entry control system, guard dogs, or other security devices.
- Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack planning activities.
- Persons drawing schematics and taking detailed notes of a dam or levee and its associated key features.

Activity Indicators (observed or reported):

- Repeated attempts from the same location or country to access protected computer information systems.
- Successful penetration and access of protected computer information systems, especially those containing information on logistics, procedures, shipment schedules, security measures, passwords, and other sensitive information.
- Attempts to obtain information about the dam or levee (e.g., blueprints of buildings, security measures or personnel, entry points, access controls, or information from public sources).
- Unfamiliar cleaning crews or other contract workers with passable credentials, or crews or contract workers attempting to access unauthorized areas.*
- A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
- Increased interest in a facility's outside components (i.e., an electrical substation not located onsite and is heavily protected or not protected at all).
- Sudden increases in power outages. Outages could be implemented from an offsite location to test the backup systems or recovery times of primary systems.
- Increase in buildings, fence gates, gate controls (e.g., spillway, intake structure), safety devices (e.g., piezometers, inclinometers, relief wells) being left unsecured or doors left unlocked that are normally locked at all times.*
- Arrest of unknown persons by local police at or near the facility. This would be more important if the asset is located in a rural area rather than in or around a large city.
- Traces of explosive or radioactive residue on vehicles during security checks by personnel using detection swipes or devices.
- Increase in violations of security guard standard operating procedures for staffing key posts.
- Increase in threats from unidentified sources by telephone, by postal mail, or through the email system.

- Increase in reports of threats from outside known, reliable sources.
- Sudden losses or theft of guard force communications equipment.
- Displaced or misaligned manhole covers or other service access doors on or surrounding the asset site.
- Unusual maintenance activities (e.g., road repairs) near the asset.
- Observations of unauthorized personnel collecting or searching through trash.*
- Unusual packages or containers, especially near pumping stations; gates; and heating, ventilation, and air conditioning (HVAC) equipment or air-intake systems.
- Unusual powders, droplets, or mist clouds near pumping stations, gates, and HVAC equipment or air-intake systems.
- Packaging and/or packaging components that are inconsistent with the usual shipping mode.
- Delivery of equipment or materials that is unexpected, unusual, out of the norm, without explanation, or with suspicious or missing paperwork.
- Excessive requests or interest in access for deliveries or pickups.
- Vendors or suppliers make unusual requests concerning the shipping or labeling of deliveries.

Suspicious Activity

Suspicious activity is any unusual behavior (i.e., outside of a normal baseline) that could indicate planning for a terrorist attack or other criminal activity. Sample categories of suspicious activity include defined criminal activities and potential terrorism nexus activities, as listed in the callout box. In addition, several types of suspicious activity may be considered innocent and therefore require additional vetting before determining if there is a reason to investigate. When observing and considering to report suspicious activity, personnel should note that race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion.

Defined Criminal Activities and Potential Terrorism Activities:

- Attempted breach or intrusion
- Aviation activity
- Cyberattack
- Expressed or implied threat
- Misrepresentation
- Sabotage, tampering, or vandalism
- Theft, loss, or diversion

Activities Requiring Additional Vetting:

- Acquisition of expertise
- Eliciting information
- Materials acquisition or storage
- Observation or surveillance
- Photography
- Recruiting or financing
- Testing or probing of security
- Weapons collection or discovery

Indicators of Suspicious Activity

In targeting critical infrastructure, potential adversaries can employ a wide range of weapons, tools, and tactics, including the use of explosives or a cyber-attack. Dams can be attractive targets because of the potential for dramatic effects and high consequences, such as downstream damage and casualties from flooding and the loss of project-specific benefits. The suspicious activity indicators listed below, while not all-inclusive, are a representative sampling of warning signs compiled from a review of terrorist events over several years.

Workplace Violence Activities Indicators:

- Sudden and dramatic changes in home life, personality, or work performance.
- Increasingly erratic, unsafe, or aggressive behaviors, including any statements or behaviors indicative of suicidal or homicidal ideations.
- Exaggerated or violent gestures (e.g., clenching fists or jaws could be interpreted as threatening or intimidating).
- Using abusive language that a reasonable person might find threatening.
- Expressed or implied threats to commit an act of violence or destruction, including observable grievances with threats and plans of retribution.
- Hostile feelings of injustice or perceived wrongdoing.
- Contextually inappropriate statements about harming others.
- Contextually inappropriate and recent acquisition of multiple weapons and/or weapons training.
- Contextually inappropriate and intense interest or fascination with previous shootings or mass attacks.

Explosives Activities Indicators:

- Explosives thefts or sales of unusual amounts of black and/or smokeless powder, blasting caps, binary explosive targets, or high-velocity explosives.
- Unusual amounts of high-nitrate fertilizer sales to non-agricultural purchasers or abnormal amounts to agricultural purchasers.
- Unusual theft/sales of combinations of ingredients for explosives (e.g., fuel oil, nitrates, peroxides, chlorates and high-concentration acids) beyond normal use.
- Theft/sales of containers (e.g., propane bottles) or vehicles (e.g., trucks, cargo vans) in combination with other indicators.
- Reports of explosions (potentially a pre-testing activity).
- Rental of self-storage space for the purpose of storing chemicals.
- Modification of a truck or van with heavy-duty springs to handle heavier loads.
- Treatment of chemical burns or missing hands or fingers.
- Untreated chemical burns or missing hands or fingers.

Weapons Activities Indicators:

- Theft or unusual sales of large numbers of semi-automatic weapons.
- Theft or unusual sales of ammunition capable of being used in military weapons.
- Reports of automatic weapons firing.
- Seizures of modified weapons or equipment used to modify weapons (e.g., silencers).
- Theft, unusual sale, or seizure of night-vision equipment or body armor.
- Reports of individuals pacing off distances from known points, as a potential threat indicator for the possible use of an “Indirect Weapons System” being employed against the facility or site.

Cyber Activities Indicators:

- The availability of the organization’s system or website has been disrupted.
- Employees, customers, suppliers, or partners are unable to access the organization’s system or website.
- The project’s service has been denied to its users.
- Persons attempting to gain information in person, by phone, or via mail or email regarding the configuration and/or cyber security posture of the organization’s website, network, software, or hardware.
- Persons attempting (either failed or successful) to gain unauthorized access to the organization’s system or its data.
- Unauthorized changes or additions to the organization’s system's hardware, firmware, or software characteristics without the IT department’s knowledge, instruction, or consent.
- Anomalies in control system behavior and alarming.
- Delivery of suspicious emails that include unsolicited attachments and/or requests for sensitive personal information, types of control system components used, software versions, or organizational information.

- Delivery of suspicious emails that include links to websites intended to mirror or replicate a vendor's website, urging system administrators or control system engineers to push patches or updates to systems.
- Unauthorized persons using the organization's system for the processing or storage of data.
- Former employees, customers, suppliers, or partners still using the organization's system.

Reporting Incidents

Suspicious activity reporting is the official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. Timely reporting helps local authorities act quickly to identify potential threats and can provide an indicator of national-level activities against similar facilities or operations. Several resources are available to help owners and operators develop a reporting program and foster a culture of reporting suspicious activity.

Describe what you saw:

- **WHAT** did you observe? Be specific.
- **WHO** did you see?
- **WHEN** did you see it?
- **WHERE** did you see this occur?

Facility personnel should take the following steps to report suspicious activity:

- Maintain awareness of the environment. This includes in or near entry or exit points, parking areas, restricted areas, and in the immediate vicinity.
- Identify behaviors that are out of the ordinary, such as the indicators of surveillance and suspicious activity described earlier in this guide.
- Report the activity to local law enforcement with as much detail as possible, using whatever means are available (e.g., take a picture with your cell phone camera, write down a note on a scrap piece of paper).

In general, the recording and reporting methods are less important than the timeliness of the report. A delayed report may mean that the subjects have left the area and authorities have subsequently lost the opportunity to identify and question them.

Type of Incidents and Information to Report

Each incident report should include the following information with as much detail possible:

- Date and time of incident
- Number of individuals involved
- Type of incident
- Description of the incident, including the location and observed behavioral indicators
- Video and/or photographs of the incident
- Past incidents or a summary of previous incidents
- Name and address of the facility
- Contact information of the individual submitting the report

Table 1 on the next page includes additional details to report about the suspect and any equipment, vehicle, aircraft, or marine vessel associated with the suspicious activity.

It is also important to protect the rights of U.S. persons by ensuring personal information is not disseminated or disclosed to anyone who does not have the authority and need to access such information. If personally identifiable information—defined as any information about an individual that can be used to distinguish or trace an individual's identity (e.g., name, social security number, date of birth, mother's maiden name, biometric records)—cannot be protected, these details should be omitted from the report.

Table 1. Types of information to include in a suspicious activity report

Suspicious Persons

- Names, aliases (including variations in spelling)
- Gender
- Physical description
- Reason for being in the area or conducting the suspicious activity
- Place of employment
- Copy of picture identification
- History of incidents of this kind involving this individual, especially at this facility

Race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion, but attributes may be documented in specific suspect descriptions for identification purposes.

Suspect's Surveillance Equipment

- Make and model of binoculars, camera, or recording equipment
- Subject and number of pictures taken
- Copy of pictures, if available

Always follow applicable laws and policies to avoid unlawful search and seizure of persons and their possessions.

Vehicles

- Color, make, model, and year
- License plate and state
- Distinguishing marks, stickers, and embellishments on the vehicle
- Any history involving the same vehicle at this location or facility

Aircraft

- Color scheme, make, model, year, and tail number
- UAS description and direction headed

Marine Vessels

- Registration identification, color, and identifying information

Other

- Description of any other suspicious individuals in the vicinity
- Description of information sought or obtained
- Names of local law enforcement or other federal, state, or local agencies that have been notified

Cyber Incident and Indicators Reporting

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of an organization's enterprise IT system or industrial control system. Organizations are encouraged to report cyber incidents and indicators, including the following:

- Significant loss of data, system availability, or control of systems.
- Attempts to gain unauthorized access to a system or its data.
- Malicious code (e.g., viruses, worms, bots) that disrupts service, steals sensitive information, or gains access to private computer systems.
- Phishing campaigns, including successful or attempted spear phishing of executives, executive assistants, control system engineers, IT administrators, or other privileged users.
- Cyber threat indicators, including malicious reconnaissance, anomalous activity that appears to indicate the existence of a security vulnerability, exploitation of a security vulnerability, or malicious cyber command and control.

When preparing to report a **cyber incident**, gather the following information:

- Date and time of when the incident started
- Date and time of when the incident was detected
- Incident description
- If the confidentiality, integrity, and/or availability of your organization's information systems is potentially compromised

When preparing to report a **cyber threat indicator**, gather the following information:

- Indicator description
- Internet Protocol (IP) address observable(s), including the IP address, port, and protocol
- Email observable(s), including sender, if the sender was spoofed, subject, and body
- Applicable kill chain stages, such as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objective
- Defensive measures deployed
- Attack patterns
- Vulnerabilities

Recipients of Suspicious Activity Reports

Many organizations have a documented process for reporting suspicious activity, which typically includes submitting a spot report to the security shift leader, notifying a supervisor, and/or submitting a formal suspicious activity report. Absent a formal policy, or in addition to reporting internally, personnel can contact local law enforcement or the FBI office. The agency contact table located at the beginning of this guide can be completed and posted in the facility for easy reference. Owners and operators should build relationships with these agencies prior to an incident to increase the efficacy of the response effort.

Dams Sector partners are encouraged to report computer or network vulnerabilities to CISA Central, to help serve as part of an early-warning system in the event the attack is targeting multiple facilities and/or sectors. CISA Central serves as the Cybersecurity and Infrastructure Security Agency's (CISA) coordinator of situational awareness and response to national cyber, communications, and physical incidents. The United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) can also be accessed via CISA Central. To report an incident, visit www.us-cert.cisa.gov/report. CISA Central can be reached by telephone at (202) 282-9201 or by email at Central@cisa.dhs.gov.

To further strengthen sector security and resilience, Dams Sector partners may also opt to report incidents and suspicious activity (physical or cyber) to a sector-specific Information Sharing and Analysis Center (ISAC), such as the WaterISAC or Electricity ISAC (E-ISAC). Notifying an ISAC can help industry analysts identify threats and vulnerabilities, communicate with partners to maintain situational awareness, and shape products and services to help partners stay safe and secure.

Resources for Reporting Incidents

A **SAR template** is included in Appendix A for easy reference. Organizations with a documented reporting process should follow the established procedure for submitting the required form. In addition, organizations should comply with applicable federal or state reporting requirements. Otherwise, the template can be used by organizations to develop or in lieu of an established process.

To help organizations mitigate potential risks in today's dynamic and rapidly evolving threat environment, CISA provides a compendium of resources for **securing public gatherings**. These resources—organized by stakeholder type such as owners and operators and first responders—address numerous threats of interest to the Dams Sector, including unauthorized access to facilities, cybersecurity, active shooter, bombings, and unmanned aircraft systems (UAS). Available resources include guides, fact sheets, posters, and training opportunities on mitigating these threats and on identifying and reporting suspicious behavior. Additional information can be found online at www.cisa.gov/securing-public-gatherings.

The DHS **"If you See Something, Say Something®" campaign** is an initiative that encourages individuals across the Nation to be the eyes and ears for safer communities. The more observant and involved individuals are in their daily lives, the less likely crime will occur undetected. Resources available to partners through this campaign include posters, pocket cards, and videos to encourage the reporting of suspicious activity. For more information on the campaign visit www.dhs.gov/see-something-say-something or send an email to SeeSay@hq.dhs.gov.

The **Nationwide Suspicious Activity Reporting Initiative** (**NSI**) is a joint effort by DHS; the FBI; and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with a tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country and also serves as the unified focal point for sharing SAR information. Additional information can be found online at www.dhs.gov/nsi.

DHS recognizes that communities are the first line of defense in keeping the public safe and secure and encourages organizations, through the **Hometown Security program**, to *Connect, Plan, Train, and Report*. Applying these four steps in advance of an incident or attack can help better prepare organizations and their employees to proactively think about the role they play in the safety and security of their operations and communities. Through this program, DHS provides free tools and resources pertaining to insider threat mitigation, counter-improvised explosive device information, the DHS Cybersecurity Awareness Campaign, tips from US-CERT, the "If you See Something, Say Something®" campaign, the NSI, and much more. Additional information can be found online at www.cisa.gov/hometown-security.

Countering Surveillance and Suspicious Activity

Effective critical infrastructure risk management to maintain operations and delivery of services depends on the ability of owners and operators to understand the risks to their facilities and operations and integrate a wide range of activities to manage those risks. Recognizing and mitigating surveillance and suspicious activity by a potential adversary is an important aspect of risk management. This chapter includes a number of actions that owners and operators can take to potentially disrupt these steps in the attack planning cycle. This is not an all-inclusive list of security and protective measures to prevent or respond to suspected surveillance or suspicious activity. Refer to other Dams Sector publications at www.cisa.gov/dams-sector-publications for additional information on crisis management planning and physical and cybersecurity actions to increase a facility's security posture.

Surveillance Detection and Counter-Surveillance

Owners and operators may opt to assign roles and responsibilities to specific personnel and/or security teams to identify and take action to counter surveillance and suspicious activity. Commonly referred to as surveillance detection and counter-surveillance, associated activities include the following:

- **Surveillance detection** is a defensive security measure used to determine whether surveillance is being conducted on your facility. Surveillance detection can be conducted temporarily by an individual or full-time by a trained team to observe, detect, and report suspicious activities. Techniques include studying activity at and near the facility; understanding what activity is normal and not normal; and gathering descriptive information about suspicious persons, vehicles, and activities.
- **Counter-surveillance** is not only used to determine whether surveillance is being conducted, but it also includes actions or techniques designed to hinder or prevent the surveillance. Counter-surveillance is usually conducted by a trained team and includes leveraging technology to detect hidden cameras or listening devices, scramble signals, or generate white noise to prevent the recording of voices.

Surveillance detection operations should not be confused with counter-surveillance operations, which may involve more direct measures by trained security or intelligence professionals to counteract hostile surveillance. However, surveillance detection and counter-surveillance operations can be implemented concurrently. Discriminating between the benign and malicious activities takes careful observation skills, patience, and practice.

Planning, Training, and Exercises

Take the time now to plan how the organization will handle a security event should the attacker succeed in advancing the attack planning cycle from surveillance steps to execution. Develop plans—including security, emergency response, communications, recovery, and continuity—that take into account the protection of employees, customers, and critical assets and any regulatory requirements, operational needs, and security measures.

In addition to the roles and responsibilities of security personnel in detecting surveillance or suspicious activity outlined above, all site personnel can be trained to detect and report possible instances of surveillance. Each person assigned to the facility should be aware of his/her role as an active observer, cognizant of his/her entire environment, and instructed to record observations and quickly report suspicious activities. Planning and training efforts should not only help employees

observe and evaluate suspicious behaviors, but also empower them to mitigate potential risk and obtain help when necessary. For example, an employee approaching an unknown individual and simply saying "Hello" can prompt a casual conversation, help to determine why they are there, and possibly deter the threat by identifying the individual and taking action to report suspicious activity. This practice is refered to as the OHNO approach—Observe, Initiate a Hello, Navigate the Risk, and Obtain Help.

While planning is essential for effective incident response, more complete preparation requires periodic exercises that test implementation of those plans. Exercises constitute a natural mechanism to maintain operational readiness by validating each plan's workability and efficiency, ensuring the plan is up to date, and recommending updates based on the exercise's findings and lessons learned. Exercises also provide a unique opportunity to test the communication protocols required to engage employees, external entities, and stakeholders.

Protective Measures

Technology Solutions

Investmenting in and deploying security technology can be useful in identifying and mitigating surveillance attempts. Closed-circuit television and thermal imagers can be used by security forces to monitor the facility for suspicious activity. When considering ideal locations for these assets, it is important to overlap surveillance coverage to maximize the opportunity to detect threats. This also compensates for other factors, such as restricted viewing angles or differences in lighting. Barriers, whether for vehicles or watercraft, can create a distance between the adversary and critical assets.

Random Anti-Terrorism Measures

Random anti-terrorism measures (RAM) include changing procedural security to make it harder for a potential adversary to use hostile surveillance to gauge the vulnerabilities associated with the facility. Examples include conducting random vehicle searches, identification checks, and facility patrols. By introducing uncertainty, a break in the normal routine can make it difficult for terrorists to identify and plan to defeat security procedures. It also elevates the risk of the adversary being identified or caught. When conducting these measures, it is important to be as overt and visible as possible to ensure there is no doubt to any onlookers that the facility is conducting a security measure.

Unmanned Aircraft System Mitigation and Security

Recognizing and implementing security practices that meet federal, state, and local regulatory requirements are key to successfully managing potential security incidents associated with UAS. Although no single solution will fully mitigate the risk from an adversary using UAS to plan or carry out an attack, consider the following measures to address UAS-related security challenges:

- Research and implement legally approved counter-UAS technology.
- Know the air domain around the facility and who has authority to take action to enhance security.
- Contact the Federal Aviation Administration to consider UAS restrictions in close proximity to fixed site facilities.
- Update Emergency/Incident Action Plans to include UAS security and response strategies.
- Build federal, state, and local partnerships to share information and aid response efforts.
- Report potential UAS threats to your local law enforcement agency.

As organizations are increasingly integrating UAS into operational functions, the following practices can lower the cybersecurity risks associated with the use of this technology:

- Ensure that the devices used for the download and installation of UAS software and firmware do not access the enterprise network.
- Download software from properly authenticated and secured websites.
- Run all downloaded files through an up-to-date antivirus platform before installation and ensure the platform remains enabled throughout installation.
- Ensure that communications are secure while operating the UAS by using encryption, enabling the highest standard of Transport Layer Security protocol that the UAS supports, and disabling connections between the UAS and the Internet.
- Erase all data from the UAS and any removable storage devices after each use.

Insider Threat Mitigation

Successful insider threat mitigation programs employ practices and systems that limit or monitor access across organizational functions. Those practices and systems, in turn, limit the amount of damage an insider can do, whether the act is intentional or unintentional. Effective insider threat mitigation programs need to be able to detect and identify improper or illegal actions, assess threats to determine levels of risk, and implement solutions to manage and mitigate the potential consequences of an insider incident. Successful insider threat mitigation programs accomplish these objectives while addressing three core principles:

- Promote a protective and supportive culture throughout the organization.
- Safeguard organizational valuables while protecting privacy, rights, and liberties.
- Remain adaptive as the organization evolves and its risk tolerance changes.

Cyber Defensive Measures

Defensive measures are any action, device, procedure, signature, or technique applied to an information system or information to detect, prevent, or mitigate a known or suspected cybersecurity threat or security vulnerability. Ranging in complexity, defensive measures include installing a security device that protects or limits access to a company's computer infrastructure to sophisticated software tools used to detect and protect against anomalous and unauthorized activities on a company's information system. Advisories issued by ICS-CERT can be helpful to understand security vulnerabilities in specific vendor products and defensive measures to take as a result.

Examples of defensive measures that could be implemented in response to suspicious activity on an organization's network include the following:

- Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls and isolate them from the business network. When remote access is required, use secure methods, such as Virtual Private Networks.
- Restrict access to devices following a least privilege principle.
- Implement physical security controls to mitigate unauthorized physical access.
- Load a signature into the organization's intrusion detection system to detect a spear phishing campaign with particular characteristics.
- Run a firewall rule that disallows a type of malicious traffic from entering a network.

Appendix A. Sample Suspicious Activity Report

Suspicious Activity Report **(insert marking designation)**		
Report Information		
Reported By:	Name Agency/Division Phone Number Email Address	
Report Date:		
Has this report been shared with other agencies?	If yes, list the agency/organization title	
Incident Information		
Location:		
Date and Time:		
Type:	☐ Aviation Activity ☐ Breach or Attempted Intrusion ☐ Eliciting Information ☐ Expressed or Implied Threat ☐ Observation or Surveillance ☐ Photography	☐ Sabotage, Tampering, Vandalism ☐ Testing or Probing of Security ☐ Theft, Loss, or Diversion ☐ Weapons Discovery ☐ Other _____
Summary:		
Action(s) Taken:		
Previous Incidents		
Has an incident of any kind occurred here before?		
Summary of Previous Incident:		

Appendix B. Acronyms

CISA	Cybersecurity and Infrastructure Security Agency
DHS	U.S. Department of Homeland Security
FBI	Federal Bureau of Investigation
GCC	Government Coordinating Council
HVAC	heating, ventilation, and air conditioning
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
IT	information technology
NSI	Nationwide Suspicious Activity Reporting Initiative
RAM	random anti-terrorism measures
SAR	suspicious activity report
SCC	Sector Coordinating Council
UAS	unmanned aircraft system
US-CERT	United States Computer Emergency Readiness Team

Appendix C. Bibliography

New York Department of Homeland Security and Emergency Services. Learn How to Spot Suspicious Activity: The Eight Signs of Terrorism Webpage. Accessed July 13, 2021. http://www.dhses.ny.gov/oct/safeguardNY/8signs.cfm.

United States Air Force, Operations Security Antiterrorism Office. "Random antiterrorism measures change base security profile", April 2006. Accessed July 13, 2021. https://www.afmc.af.mil/News/Commentaries/Display/Article/155902/random-antiterrorism-measures-change-base-security-profile/.

United States Air Force, Office of Special Investigations Webpage. Accessed July 13, 2021. https://www.osi.af.mil/.

U.S. Department of Justice, Bureau of Justice Assistance, Office of Justice Programs. *10 Ways to Integrate Suspcious Activity Reporting into your Agency's Operations*, January 2017. Accessed July 13, 2021. https://www.dhs.gov/sites/default/files/publications/17_0315_NSI_10-Ways-Integrate-SSAR-Into-Agencys-Operations.pdf.

U.S. Department of Justice, Bureau of Justice Assistance, Office of Justice Programs. *Suspicious Activity Reporting: Process Implementation Checklist*, January 2017. Accessed July 13, 2021. https://www.dhs.gov/sites/default/files/publications/17_0315_NSI_SAR-Process-Implementation-Checklist.pdf.

U.S. Department of Justice, Federal Bureau of Investigation, *Agricultural, Chemical, and Petroleum Industry Terrorism Handbook,* 2006. Accessed July 13, 2021. https://www.hsdl.org/?abstract&did=471463.

U.S. Department of Justice, Offices of the United States Attorneys. Pre-Incident Indicators Webpage, last updated November 3, 2020. Accessed July 13, 2021. https://www.justice.gov/usao-edwi/anti-terrorism-advisory-council.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Connect, Plan, Train, Report Webpage. Accessed July 13, 2021. https://www.cisa.gov/connect-plan-train-report.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. *Counter-IED Resources Guide*, March 2017. Accessed July 13, 2021. https://www.cisa.gov/publication/obp-counter-ied-resources-guide.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. *Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems*, June 2019. Accessed July 13, 2021. https://www.cisa.gov/publication/cybersecurity-best-practices-operating-commercial-unmanned-aircraft-systems.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Dams Sector Publications Webpage. Accessed July 13, 2021. https://www.cisa.gov/dams-sector-publications.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Employee Vigilance – Power of Hello Webpage. Accessed July 13, 2021. https://www.cisa.gov/employee-vigilance-power-hello.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Hometown Security Tools and Resources Webpage. Accessed July 13, 2021. https://www.cisa.gov/tools-and-resources.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Insider Threat – Cyber Webpage. Accessed July 13, 2021. https://www.cisa.gov/insider-threat-cyber.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Insider Threat Mitigation Webpage, last updated November 18, 2020. Accessed July 13, 2021. https://www.cisa.gov/insider-threat-mitigation.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Report Incidents, Phishing, Malware, or Vulnerabilities Webpage. Accessed July 13, 2021. https://us-cert.cisa.gov/report.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Securing Public Gatherings Webpage. Accessed July 13, 2021. https://www.cisa.gov/securing-public-gatherings.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Unmanned Aircraft Systems (UAS) – Critical Infrastructure Webpage. Accessed July 13, 2021. https://www.cisa.gov/uas-critical-infrastructure.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Unmanned Aircraft Systems (UAS) Frequently Asked Questions Webpage. Accessed July 13, 2021. https://www.cisa.gov/unmanned-aircraft-systems-faq.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. US-CERT DHS Cyber Threat Indicator and Defensive Measure Submission System Webpage. Accessed July 13, 2021. https://us-cert.cisa.gov/forms/share-indicators.

U.S. Department of Homeland Security, Federal Emergency Management Agency. Dam Safety Website, last updated December 7, 2020. Accessed July 13, 2021. https://www.fema.gov/emergency-managers/risk-management/dam-safety.

U.S. Department of Homeland Security. *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*. Accessed July 13, 2021. https://www.dhs.gov/publication/cyber-incident-reporting-unified-message-reporting-federal-government.

U.S. Department of Homeland Security. If You See Something, Say Something® Webpage. Accessed July 13, 2021. https://www.dhs.gov/see-something-say-something.

U.S. Department of Homeland Security. *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5*, February 2015. Accessed July 13, 2021. https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional-Standard-SAR.pdf.

U.S. Department of Homeland Security. Nationwide SAR Initiative Webpage. Accessed July 13, 2021. https://www.dhs.gov/nsi.

U.S. Department of Homeland Security. *Protect Your Workplace: Guidance on Physical and Cyber Security and Reporting of Suspicious Behavior, Activity, and Cyber Incidents*, February 2006. Accessed July 13, 2021. https://us-cert.cisa.gov/sites/default/files/publications/brochure_securityguidance.pdf.

U.S. Department of Homeland Security. *Recognize the Signs of Terrorism-Related Suspicious Activity*, July 2018. Accessed July 13, 2021. https://www.dhs.gov/sites/default/files/publications/18_0701_seesay_indicatorinfographic.pdf.

U.S. Department of Homeland Security. *Suspicious Activity Reporting Indicators and Examples*, March 2018. Accessed July 13, 2021. https://www.dhs.gov/sites/default/files/publications/18_0531_NSI_SAR-Indicators-Examples.pdf.

U.S. Department of Homeland Security. What is Suspicious Activity Webpage. Accessed July 13, 2021. https://www.dhs.gov/see-something-say-something/what-suspicious-activity.

U.S. Department of Homeland Security and U.S. Department of Justice. *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*, October 2020. Accessed July 13, 2021. https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance.

U.S. Food and Drug Administration. CARVER + Shock Primer Webpage. Accessed July 13, 2021. https://www.fda.gov/food/food-defense-programs/carver-shock-primer.

Water Information Sharing and Analysis Center. Report Incidents and Suspicious Activity to WaterISAC and Authorities Webpage. Accessed July 13, 2021. https://www.waterisac.org/report-incidents-and-suspicious-activity-waterisac-and-authorities.