Surveillance and Suspicious Activity Indicators Guide for Dams and Levees

November 2017

Homeland Security

This page is intentionally blank.

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 (PSA)		
DHS Cybersecurity Advisor (CSA)		
DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)		
Local Joint Terrorism Task Force (JTTF)		
Local Federal Bureau of Investigation (FBI)		
FBI Weapons of Mass Destruction (WMD) Coordinator		
FBI Hotline		
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		
Local Response Diving Unit		
Local Response Bomb Squad		

ACKNOWLEDGEMENTS

This document was developed with input, advice, and assistance from the Dams Sector Security Education Working Group (SEWG), Levee Subsector Council and members of the Dams Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC), which included representatives from the public and private sector. For a complete list of member organizations, visit https://www.dhs.gov/dams-sector-council-charters-and-membership. The *"Surveillance and Suspicious Activity Indicators Guide for Dams and Levees"* provides members of the Dams Sector with the capability to report and retrieve information pertaining to suspicious activities that may potentially be associated with pre-incident surveillance, activities exploring or targeting a critical infrastructure facility or system, or any possible violation of law or regulation that could compromise the facility or system in a manner that could cause an incident that would jeopardize life or property.

IP Cover Photo Location: The Dalles Dam, Oregon

Distribution

This *2016 Surveillance and Suspicious Activity Indicators Guide for Dams and Levees* was prepared under the auspices of the U.S. Department of Homeland Security. For distribution information, contact dams@hq.dhs.gov.

Notice

This material does not constitute a regulatory requirement nor is it intended to conflict, replace, or supersede existing regulatory requirements or create any enforcement standard.

INTRODUCTION

The purpose of this guide is to provide information for dam and levee owners and operators on issues related to potential terrorists' surveillance objectives, indicators that such surveillance may be taking place and methods for reporting incidents of surveillance or suspicious activity.

Like all critical infrastructures, the technological and national security environment in which the U.S. dam infrastructure is operated and maintained continues to evolve. New threats to the continued reliability and integrity of all infrastructures require vigilance. Areas of possible focus by owners and operators include: surveillance detection, identification of site-related vulnerabilities (e.g. access control, operational security and cybersecurity measures), emergency response/prevention issues and functionality issues governed by interdependencies with other infrastructure assets.

The Dams Sector comprises the assets, systems, networks, and functions related to the Nation's dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other water control facilities. Dam projects are complex facilities that typically include water impoundment or control structures, reservoirs, spillways, outlet works, powerhouses, and canals or aqueducts. In some cases, navigation locks are also part of the dam project.

Levees are embankments that may have appurtenant structures such as closure and draining devices and pumps. Though generally earthen embankments, levees can be constructed of concrete or steel. They are designed and constructed to contain, control, or divert the flow of water so as to provide protection from temporary flooding.

To address security issues related to dams and levees and the other assets within the Dams Sector, a partnership approach has been adopted involving Federal, State, regional, territorial, local, or tribal government entities; private sector owners and operators and representative organizations; academic and professional entities; and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's critical sector assets.

The goals of this guide are to enhance the security posture of dams and levees by providing information to owners and operators on:

1. ***Surveillance objectives,***
2. ***Surveillance/Suspicious activity indicators, and***
3. ***Reporting incidents of surveillance/suspicious activity.***

ATTACK CYCLE

The initial step in the attack cycle (Figure 1) process is to identify and select a target. Often, an adversary will choose a target and then plan a method of attack based on the target's vulnerabilities. While selecting a target and formulating an attack method, adversaries will conduct detailed surveillance of the area to assess security measures and identify physical barriers (i.e. fences, access restrictions, etc.). Surveillance assists the adversary in determining if the attack will be successful or not. Additionally, an adversary's repeated appearance at a target may indicate the adversary is assessing if Random Access Measures (RAM's) have been employed and determining if something changed which could impact the attack plan (e.g. new barriers placed, guards being posted at varying hours, K-9 patrols, etc.). Planning and rehearsals are conducted to improve the odds of success, confirm planning assumptions, and develop contingencies.

In targeting critical infrastructure, potential adversaries can employ a wide range of weapons, tools, and tactics, including the possible use of explosives. Some adversaries could potentially use less traditional methods, such as cyber-attacks. Attacks of this nature would involve using digital control and information systems to deny, exploit, corrupt, or destroy a target's operational capabilities. 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. Once sufficient surveillance, rehearsal and planning have been conducted, the attack will be deployed. If the attack was properly planned, the attack is very likely to succeed. The attack cycle is generally representative of an adversary's process. An actual event may happen in a more compressed schedule and with fewer steps. 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.

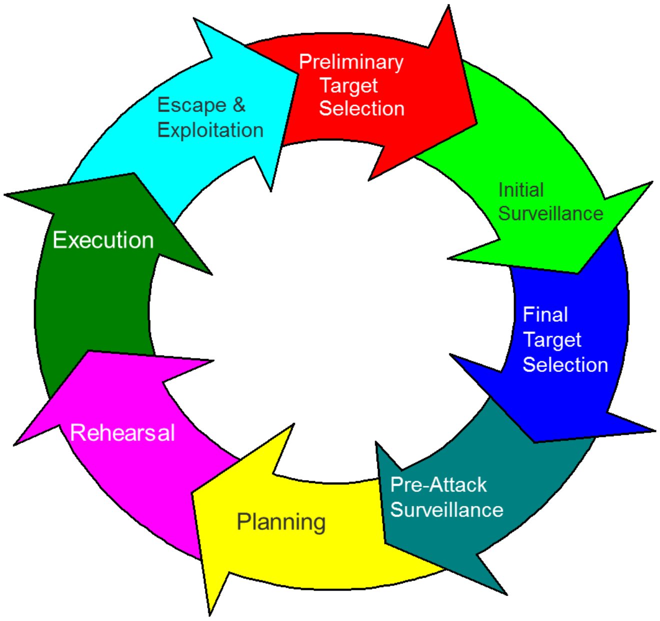

Figure 1: The Attack Cycle

OBJECTIVES OF CRITICAL INFRASTRUCTURE SURVEILLANCE

The overall objective of surveillance activity is to determine possible targets, attack modes and the likelihood of success of an attack against a critical infrastructure asset. An adversary's specific surveillance objectives could be to identify 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; and
- Places where further surveillance can take place.

Potential adversaries engage in surveillance activities to identify any security vulnerabilities that can be exploited. In trying to identify security vulnerabilities, potential adversaries may conduct sophisticated surveillance over a long period of time—months or years—which can be highly effective, but difficult to detect. After surveillance of a target has concluded and preparations for the attack are complete, a final pre-attack surveillance may be done to determine whether changes in surroundings or conditions will impact carrying out a successful attack.

Surveillance can be fixed or mobile. Mobile surveillance consists of driving by a site to observe the facility or site operations. Surveillance can also be accomplished in the air with the use of Unmanned Aircraft Systems (UAS) – see Appendix C. With regards to levees, mobile surveillance would most commonly be done by driving or walking the length of a levee 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 surveillance activity might include the repeated presence of an unfamiliar vehicle in the area, the presence of UAS or persons walking on or around the levee for reasons that do not seem obvious.

Fixed surveillance might be more typical for dams. Fixed surveillance is done from a static, often concealed position. Adversaries may establish themselves in a public location over an extended period of time, such as a recreational area close to a dam. They may also pose as a fisherman, tourists, delivery person, photographers, or even demonstrators to provide a plausible reason for being in the area.

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 personnel and/or law enforcement.

Modern technologies available to consumers should be considered during all forms of surveillance, such as night vision cameras, UAS, telescopic lenses and hackers capable of breaching the dam's security systems. Surveillance also includes the indirect means of gathering the information, such as recruitment of employees, either voluntary or involuntary or eliciting or conning information about the dam from employees or venders who have access to various locations within or around the facility.

It is important to note that 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 suspicions. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

Indicators that surveillance activities might be taking place have been developed by DHS and law enforcement agency partners. Awareness of these indicators can contribute to an asset's security posture.

INDICATORS OF POSSIBLE SURVEILLANCE

Indicators that an asset may be under surveillance include recognizing that the normal environment isn’t quite right or that seemingly normal activities arouse suspicion. The following table of indicators of surveillance activity illustrates possible warning signs.

Table 1: Surveillance Indicators and Indicators of Suspicious Activity Observed at or near a Dam or Levee

	Human Indicators (Observed or Reported)
1	Persons using video/camera/observation equipment and/or UAS to take pictures or videos of infrastructure or security measures in an unusual or surreptitious manner.
2	Persons with installation maps photos, or diagrams with highlighted areas or notes regarding infrastructure or a listing of installation personnel.
3	Persons possessing or observed using night-vision devices near the levee or dam perimeter or in the local area with no apparent reasonable explanation.
4	Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
5	Nonmilitary persons seen with military-style weapons and clothing/equipment.
6	Questioning personnel off-site about practices pertaining to the dam or levee or an increase in personal email, telephone, faxes or postal mail concerning the dam or levee or its critical features.
7	Persons not associated with the dam or levee showing an increased general interest in the area surrounding it.
8	Dam or levee personnel maintain unofficial and regular contact with persons soliciting information about the levee or dam at a level beyond mere curiosity.*
9	Persons attempting unauthorized access (i.e. criminal hacking) of computers, systems, or websites looking for personal information, maps, or other targeting examples.*
10	An employee who changes working behavior or works more irregular hours without approval or a reasonable explanation.*
11	Persons observing deliveries, especially of hazardous or toxic materials.
12	Aircraft or UAS flyover in restricted airspace; boat encroachment into restricted areas, especially if near a critical infrastructure.
13	A noted pattern or series of false alarms requiring a response by law enforcement or emergency services.
14	Theft of contractor identification cards or uniforms, or unauthorized persons in possession of identification cards or uniforms.
15	Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, CCTV, IDS, electric entry control system, guard dogs, or other security devices.
16	Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack-planning activities.
17	Persons drawing schematics and taking detailed notes of a dam or levee and its associated key features.

Activity Indicators (Observed or Reported)	
18	Repeated attempts from the same location or country to access protected computer information systems.
19	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.
20	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).
21	Unfamiliar cleaning crews or other contract workers with passable credentials; crews or contract workers attempting to access unauthorized areas.*
22	A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
23	Increased interest in a facility's outside components (i.e., an electrical substation not located on site and is heavily protected or not protected at all).
24	Sudden increases in power outages. Outages could be implemented from an off-site location to test the backup systems or recovery times of primary systems.
25	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.
26	Arrest of unknown persons by local police. This would be more important if the asset is located in a rural area rather than in or around a large city.
27	Traces of explosive or radioactive residue on vehicles during security checks by personnel using detection swipes or devices.
28	Increase in violation of security guard standard operating procedures for staffing key posts.
29	Increase in threats from unidentified sources by telephone, by postal mail, or through the e-mail system.
30	Increase in reports of threats from outside known, reliable sources.
31	Sudden losses or theft of guard force communications equipment.
32	Displaced or misaligned manhole covers or other service access doors on or surrounding the asset site.
33	Unusual maintenance activities (e.g., road repairs) near the asset.
34	Observations of unauthorized personnel collecting or searching through trash.*
35	Unusual packages or containers, especially near pumping stations, gates, and HVAC equipment or air-intake systems.
36	Unusual powders, droplets, or mist clouds near pumping stations, gates and HVAC equipment or air-intake systems.
37	Packaging and/or packaging components that are inconsistent with the usual shipping mode.
38	Delivery of equipment or materials that is unexpected, unusual, out of the norm, without explanation, or with suspicious or missing paperwork.
39	Excessive requests or interest in access for deliveries or pickups.
40	Vendors or suppliers make unusual requests concerning the shipping or labeling of deliveries.

* Also, an indicator of insider threat. For more information, see Appendix D.

Suspicious Activity Indicators

Adversaries may also engage in suspicious activities that could be indicators of a possible threat to a dam or levee. The suspicious activity indicators listed below are more likely to be known or observed by local law enforcement agencies than by owners and operators of dams and levees. This makes communication between law enforcement agents and owners and operators very important.

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 abnormally unusual 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 truck or van with heavy-duty springs to handle heavier loads.
- Treatment of chemical burns or missing hands/fingers.
- Untreated chemical burns or missing hands/fingers.

Weapons Activities Indicators

- Theft/unusual sales of large numbers of semi-automatic weapons.
- Theft/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.
- Facility owners should be cognizant 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 their facility/site.

REPORTING INCIDENTS

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another 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. More information can be found online at https://nsi.ncirc.gov.

Type of Incidents to Report

Criminal/Terrorism-Related

- Breach/Attempted Intrusion
- Misrepresentation
- Threat/Loss/Diversion
- Sabotage/Tampering/Vandalism
- Cyberattack
- Expressed or Implied Threat
- Aviation Activity

Potentially Criminal/Non-Criminal Requiring More Information*

- Eliciting Information
- Testing or Probing of Security
- Recruiting/Financing
- Photography
- Observation/Surveillance
- Materials Acquisition/Storage
- Acquisition of Expertise
- Weapons Collection/Discovery
- Sector-Specific Incident

* The nine potential criminal or non-criminal activities are not inherently criminal behaviors and may include constitutionally protected activities. Constitutionally protected activities must not be documented unless there are articulable facts or circumstances that clearly support the determination that the behavior is not innocent, but rather reasonably indicative of pre-operational planning associated with terrorism.

The Nationwide Suspicious Activity Reporting Initiative provides more information on these behaviors at: https://nsi.ncirc.gov/documents/ISE-SAR_functional_standard_indicators_and_examples_0315.pdf.

Who Should Receive Incident Reports?

DHS encourages recipients of this document to report information concerning suspicious or criminal activity to local police first and then to the FBI and DHS. Suspicious activity should also be reported via the SAR tool (Appendix A) and to the National Infrastructure Coordinating Center (NICC), which is the critical infrastructure-focused element of the DHS National Operations Center.

The NICC can be reached by telephone at (202) 282-9201 or by email at NICC@hq.dhs.gov.

The FBI regional phone numbers can be found online at www2.fbi.gov/contact/fo/fo.htm.

What Should be Reported?

- ➢ Each incident report should include the following information to the maximum level of detail possible:
  - Date and time of incident
  - Number of individuals involved
  - Type of incident
  - Description of the incident and or video and photographs
  - Past incidents / Summary of previous incidents
  - Name and address of the facility
  - Contact information of the individual submitting the report

Types of Information to 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 IDs
- ➢ History of incidents of this kind involving this individual, especially at this facility

Race, ethnicity, gender, national origin, and 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.

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
- Unmanned Aircraft Systems - See Appendix C

Marine vessels

- Registration ID, color, and identifying information

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.

Description of any other suspicious individuals in the vicinity

Names of local law enforcement or other Federal, State, or local agencies that have been notified

The Department of Homeland Security created and promotes the "See Something, Say Something" Campaign. For more information, see Appendix B.

RECOMMENDATIONS:

1. ***Complete the agency contact information in the front of this guide. Print out and post for easy access.***
2. ***Build relationships with these agencies before an incident occurs.***

Appendix A – Suspicious Activity Report

The Suspicious Activity Report (SAR) form provides members of the Dams ISE with the capability to report and retrieve information pertaining to suspicious activities that may potentially be associated with pre-incident surveillance, activities exploring or targeting a critical infrastructure facility or system, or any possible violation of law or regulation that could compromise the facility or system in a manner that could cause an incident jeopardizing life or property. The SAR form does not replace traditional reporting channels, including 911 in an emergency situation.

The SAR Tool can be accessed via the HSIN-CI/Dams Portal. Upon accessing the entry form, the system will prompt you to provide information pertaining to the suspicious activity observed. The entry form is divided into two main components: background and subject. The background section allows you to input information pertaining to the facility, type of suspicious activity, and date/time of the incident. The subject section provides the opportunity to input information pertaining to generic descriptions of the subject. Although the information may be generic, it contains sufficient data to conduct an analysis, should it be necessary. To the extent possible, it is imperative that the information submitted fully describes the suspicious activity. Supporting documentation may also be attached to the report, should you deem it necessary for the reader to better understand the incident.

Please do not include any Personal Identifiable Information (PII), which is defined as any information about an individual that can be used to distinguish or trace an individual’s identity, such as name, social security number, date of birth, mother’s maiden name, biometric records, and any other personal information that is linked or linkable to a specific individual.

Reports submitted in the SAR reporting system will automatically be available to all members of the Dams Information Sharing Environment (ISE), intelligence components from various Government and private entities, and the NICC.

Dams ISE members should consider reporting suspicious activities for the benefit of the sector. The goal is not only to enhance the sector’s information sharing capability, but also to incorporate Office of Cyber & Infrastructure Analysis (OCIA) analytical capabilities, including trend analysis, for further analysis of the information provided by members of the Dams ISE.

The SAR form is available at: **https://hsin.dhs.gov/ci/ds/Resources/DamsSARLandingPage.aspx**

Appendix B – "If You See Something, Say Something" Campaign

The Department of Homeland Security's "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. A safe community requires the joint effort of all community members. The more observant and involved individuals are in their daily lives, the less likely crime will occur undetected. If we watch and report suspicious activity, we reduce the areas where criminals feel comfortable committing crimes, resulting in safer towns and cities across the nation.

What is suspicious activity?

Suspicious activity is any observed behavior that could indicate terrorism or other criminal activity. Examples include:

Unusual items or situations: A vehicle in an odd location, unattended luggage/package, open door/window that's normally closed and locked, etc.

Eliciting information: Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security, etc.

Observation/Surveillance: Unusual attention to facilities or buildings beyond a casual or professional interest. Extended loitering without explanation, particularly in concealed locations with optimal visibility of potential targets. Unusual, repeated and/or prolonged observation of buildings (e.g., with a video camera or binoculars), taking notes and/or measurements, sketching floor plans.

Many of these activities could be innocent. Law enforcement professionals must examine suspicious behaviors in a larger context to determine whether there is reason to investigate. The activities above are not all-inclusive. They have been compiled from a review of terrorist events over several years.

Who to notify and what to report?

Report suspicious activity to a person in authority, such as local law enforcement. Don't be afraid to report something, even if you aren't sure it was serious.

Who to tell?

- On or near a dam or levee, tell security officials or the nearest facility employee.
- On the street, tell a police officer.
- On a bus, tell the driver.
- In a train or subway station, tell a security guard.

- Or, call local law enforcement.

What to tell them?

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?
- **WHY** is it suspicious?

When to report?

Report suspicious activity to local law enforcement **immediately**!

Together, we can keep our community safe. Report suspicious activity to local authorities. For more information on the "If You See Something, Say Something" campaign:

Visit: www.dhs.gov/see-something-say-something

Email: SeeSay@hq.dhs.gov

APPENDIX C – UNMANNED AIRCRAFT SYSTEMS

What is the Threat?

In addition to recreational use, unmanned aircraft systems (UAS) – also known as unmanned aerial vehicles (UAV) or drones – are used across our Nation to support firefighting and search and rescue operations, to monitor and assess critical infrastructure, to provide disaster relief by transporting emergency medical supplies to remote locations and to aid efforts to secure our borders. However, UAS can also be used for malicious schemes by terrorists, criminal organizations (including transnational organizations) and lone actors with specific objectives. UAS– related threats may include:

Weapon or Smuggling Payloads – Depending on power and payload size, UAS may be capable of transporting contraband, chemical or other explosive/weaponized payloads.

Prohibited Surveillance and Reconnaissance – UAS are capable of silently monitoring a large area from the sky for nefarious purposes.

Intellectual Property Theft – UAS can be used to perform cybercrimes involving theft of trade secrets, technologies or sensitive information.

Intentional Disruption or Harassment – UAS may be used to disrupt or invade the privacy of other individuals.

Why Is This Threat Important to Critical Infrastructure?

Since UAS use in the United States has increased as a cost-effective, versatile business and national security tool, as well as a popular recreational hobby, the Federal Aviation Administration (FAA) estimates combined hobbyist and commercial UAS sales will rise from 2.5 million in 2016 to 7 million in 2020. As a result, potential threats associated with UAS will continue to expand in nature and increase in volume in the coming years. Because of their physical and operational characteristics, UAS can often evade detection and create challenges for the critical infrastructure community.

As part of the FAA Extension, Safety, and Security Act (FESSA) of 2016, Section 2209 directs the Secretary of Transportation to establish a process to allow applicants to petition the Administrator of the FAA to prohibit or restrict the operation of an unmanned aircraft in close proximity to a fixed site facility. The fixed site facilities that are allowed to be considered include critical infrastructure, such as energy production, transmission, and distribution facilities and equipment; oil refineries and chemical facilities; amusement parks; and other locations that warrant such restrictions. For more information, visit https://www.faa.gov/uas/where_to_fly/airspace_restrictions/.

What Actions Can You Take?

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 this risk, there are several measures that can be taken 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 FAA to consider UAS restrictions in close proximity to fixed site facilities. More information can be found at www.faa.gov/uas/.
- Update Emergency/Incident Action Plans to include UAS security and response strategies.
- Build Federal, State, and local partnerships for adaptation of best practices and information sharing. More information can be found at www.dhs.gov/hometown-security.
- Report potential UAS threats to your local law enforcement agency.
- For more information, visit https://www.dhs.gov/uas-ci.

APPENDIX D – 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.

The Office of Infrastructure Protection released an “Understanding the Insider Threat” video. This video features security and behavioral subject matter experts with real-world event experience and offers recommendations to help protect organizations against this growing threat.

To access the “Understanding the Insider Threat” video, please visit the DHS Active Shooter Preparedness webpage at https://www.dhs.gov/active-shooter-preparedness. There is also an accompanying trailer that introduces the video’s concepts.

APPENDIX E – ACRONYMS

CCTV	Closed-Circuit Television
DHS	U.S. Department of Homeland Security
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FOUO	For Official Use Only
GCC	Government Coordinating Council
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
HVAC	Heating, Ventilation, and Air Conditioning
ID	Identification
IDS	Intrusion Detection System
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
NICC	National Infrastructure Coordinating Center
NOC	National Operations Center
OCIA	Office of Cyber & Infrastructure Analysis
RAM	Random Access Measures
SAR	Suspicious Activity Report
SCC	Sector Coordinating Council
SEWG	Security Education Working Group
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector-Specific Agency
UAS	Unmanned Aircraft Systems
WMD	Weapons of Mass Destruction

APPENDIX F – BIBLIOGRAPHY

(Internet sites accessed March 2017)

Federal Bureau of Investigation, Department of Justice, *Agricultural, Chemical, and Petroleum Industry Terrorism Handbook*, [http://mcpr-cca.org/downloads/FBIAgChemHandbook.pdf].

Federal Emergency Management Agency, U.S. Department of Homeland Security, *Benefits of Dams*, [http://www.fema.gov/benefits-dams].

Air Force Office of Special Investigations, U.S. Air Force, *Eagle Eyes: Categories of Suspicious Behavior*, [http://www.osi.af.mil/Home/Eagle-Eyes/].

Kentucky State Police, [http://www.kentuckystatepolice.org/terror.htm]

U.S. Department of Homeland Security, NIPP 2013 "Partnering for Critical Infrastructure Security and Resilience",[https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf].

U.S. Army Corps of Engineers, *National Inventory of Dams*, [http://nid.usace.army.mil].

U.S. Department of Homeland Security, Office of Bombing Prevention, *Counter-IED Resources Guide*, [https://www.dhs.gov/sites/default/files/publications/obp-counter-ied-resources-guide-508.pdf].

National Criminal Intelligence Resource Center, *Nationwide SAR Initiative*, [https://nsi.ncirc.gov/].

New York City Metropolitan Transit Authority, *Eight Signs of Terrorist Activity*, [http://scnus.org/resources/alerts-and-warnings/seven-signs-of-terrorist-activity].

Secure Community Network, *Terrorist Surveillance Indicators*, [http://scnus.org/resources/model-security-policies-procedures/terrorist-surveillance-indicators].

Offices of the United States Attorneys, U.S. Department of Justice, *Terrorist Surveillance Techniques*, [http://www.justice.gov/usao-edwi/anti-terrorism-advisory-council]

Developed jointly by:

Dams Sector-Specific Agency

Dams Sector Coordinating Council

Levee Sub-Sector Coordinating Council

Dams Sector Government Coordinating Council