Dams Sector Security Awareness Guide

A Guide for Owners and Operators

2007

Homeland Security

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		
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		
Department of Homeland Security (DHS) Protective Security Adviser for This State		
State Fusion Center		

Acknowledgments

The Dams Sector Coordinating Council, Dams Sector Government Coordinating Council, the Department of Homeland Security (the Dams Sector-Specific Agency), and the Critical Infrastructure Partnership Advisory Council acknowledge the active support and participation from the following security partners from the private sector: Allegheny Energy, Ameren Services Company, American Electric Power, Association of State Dam Safety Officials, AVISTA Utilities, CMS Energy, Dominion Resources, Duke Energy, Exelon Corporation, National Hydropower Association, National Mining Association (ex officio), National Water Resources Association, New York City Department of Environmental Protection, New York Power Authority, Ontario Power Generation, Pacific Gas and Electric Company, PPL Corporation, Public Utility District 1 of Chelan County, WA, Scana Corporation, South Carolina Public Service (Santee-Cooper), Southern California Edison, Southern Company Generation, TransCanada, U.S. Society on Dams, and Xcel Energy, and the following government security partners: Bureau of Reclamation (which also serves as representative for the Bureau of Indian Affairs, National Park Service, Bureau of Land Management, and other Department of Interior bureaus owning dams), Federal Energy Regulatory Commission, International Boundary Water Commission, Mine Safety and Health Administration, Natural Resources Conservation Service, Tennessee Valley Authority, U.S. Army Corps of Engineers, and State dam safety officials from California, Colorado, Nebraska, New Jersey, Ohio, Pennsylvania, Virginia, and Washington.

Distribution

This 2007 Dams Sector Security Awareness Guide was prepared under the auspices of the U.S. Department of Homeland Security. For distribution information, contact dams@dhs.gov.

Notice

Introduction

Like all critical infrastructure, the technological and national security environment in which the U.S. dam infrastructure is operated and maintained continues to evolve over time. 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 cyber security 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 dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, or other similar water retention and/or 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.

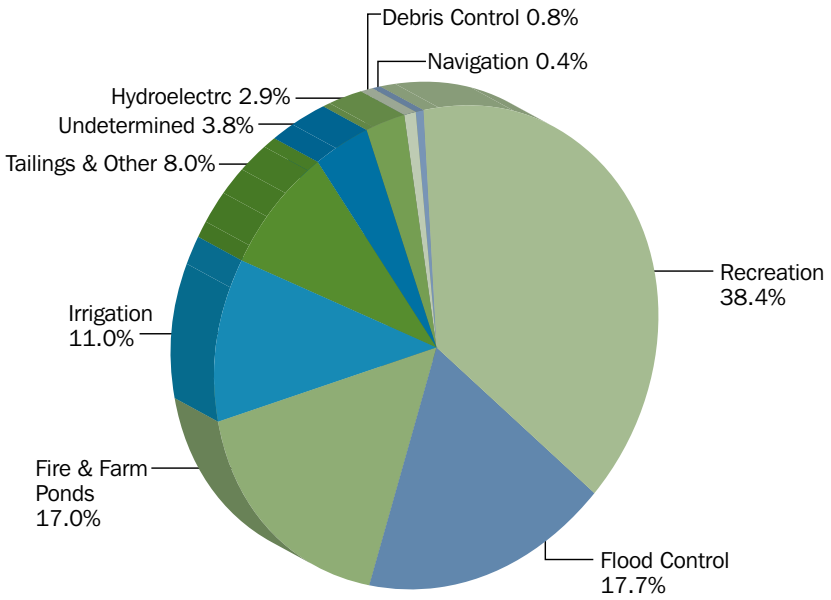
To address security issues related to dams, a partnership approach has been adopted involving Federal, State, regional, Territorial, local, or tribal government entities; private sector owners and operators and representative organizations; academic and professional entities; and certain not-for-profit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

Benefits of Dams to the Nation

The more than 82,000 dams throughout the United States and on the Nation's borders provide the country with a wide range of important economic, environmental, and social benefits. These benefits include:

- **Recreation** – Boating, skiing, camping, picnic areas, and boat launch facilities are all supported by dams.
- **Flood Control** – Dams impound floodwaters and then either release them under control to the river below the dam or store or divert the water for other uses.
- **Water Storage** – Reservoirs created by dams supply water for industrial, municipal, and agricultural uses.
- **Irrigation** – Ten percent of American cropland is irrigated using water stored behind dams; thousands of jobs are tied to producing crops grown with irrigated water.
- **Mine Tailings** – More than 1,300 mine tailing impoundments allow the mining and processing of coal and other vital minerals while protecting the environment.
- **Electrical Generation** – Dams produce more than 103,800 megawatts of clean, renewable electricity and meet up to 8 percent of the Nation's power needs.
- **Debris Control** – Some dams provide enhanced environmental protection through the retention of hazardous materials and detrimental sedimentation.
- **Navigation** – Dams and locks provide for a stable system of inland river transportation throughout the heartland of the Nation.

Figure 1-1: Distribution of Dams by Primary Purpose (Source: National Inventory of Dams, 2005)



Dams as Critical Infrastructure and Key Resources of the Nation

Because of the benefits they provide, dams are considered among the Nation's critical infrastructure and key resources (CIKR). Critical infrastructures are those assets, systems, networks, and functions that are so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, or public health or safety. Key resources are the publicly or privately controlled resources that are essential to the minimal operations of the economy and government.

The Homeland Security Act of 2002 provides the basis for the responsibilities of the Department of Homeland Security (DHS) to protect the Nation's CIKR. More specifically, DHS is the Sector-Specific Agency (SSA) with responsibilities for the Dams Sector.

The Dams Sector comprises the assets, systems, networks, and functions related to dam projects, levees, navigation locks, hurricane barriers, mine tailing impoundments, and other similar water retention or water control facilities. The Dams Sector security partners are the Federal, State, regional, territorial, local, or tribal government entities that own, operate, or regulate dams; private sector owners and operators of dams; and organizations that share in the responsibility for protecting dams.

The vast majority of the dams in the United States are privately owned and operated. The Dams Sector Coordinating Council (SCC) is the primary interface with DHS for private owners and operators on security issues related to the Dams Sector. The membership of the SCC and information on how to contact the SCC are provided in appendix A.

The Dams Sector Government Coordinating Council (GCC) is the primary interface with DHS for dams that are not privately owned. The GCC membership and contact information are available in appendix B.

The SCC and GCC partner with each other and the SSA to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for the protection of assets within the Dams Sector. This guide is an example of that partnering.

The Dams Sector Security Education Workgroup, comprising representatives of the SCC, GCC, and SSA, initiated development of the guide. The workgroup recognized that dams could be perceived as potential targets by individuals wishing to inflict harm on the Nation and that it is therefore simply prudent to maintain a security awareness posture.

The goals of this guide are to enhance dam owners' and operators' security postures by providing information on:

1. *surveillance objectives;*
2. *surveillance/suspicious activity indicators; and*
3. *reporting incidents of surveillance/suspicious activity.*

Objectives of CIKR Surveillance

The overall objective of surveillance activity is to determine possible targets, attack modes, and the likelihood of success of an attack against a CIKR asset. An aggressor'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, contractors;
- Security event response times and type of response;
- Access point locations;
- Opportunities for cascading damage effects;
- Locations and characteristics of vulnerable structural components;
- Patterns of concentration of people and vehicles; and
- Places where further surveillance can take place.

Potential aggressors engage in surveillance activities to identify any security vulnerabilities they can exploit. In trying to identify security vulnerabilities, potential aggressors may conduct sophisticated surveillance over a long period of time—months or years—which can be highly effective, but difficult to detect. In most instances, after surveillance of a target has concluded and after preparations for the attack are complete, one final pre-operational survey is typically done. This is done to determine whether changes in surroundings or conditions 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; fixed surveillance might be more typical for dams.

Fixed surveillance is done from a static, often concealed position. Aggressors may establish themselves in a public location, such as a recreational area close to a dam, over an extended period of time. They may also pose as fishermen, tourists, deliverymen, photographers, or even demonstrators to provide a plausible reason for being in the area.

Aggressors 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 continues until the aggressor determines that the asset is a suitable target. This type of transient action makes the surveillance more difficult to detect or predict.

Indicators that surveillance activities might be taking place have been developed by DHS and law enforcement agencies.

Awareness of these indicators can contribute to an asset's security posture.

Indicators of Possible Surveillance

Indicators that an asset may be under surveillance are those warning signs that the normal environment isn't quite what it should be; that seemingly normal activities seem somewhat suspicious. The following table of possible indicators of surveillance activity points out what some of those warning signs might be.

Table 1: Indicators of Possible Surveillance

Indicators About People (Observed or Reported)	
1	Persons using or carrying video/camera/observation equipment.
2	Persons with installation maps or photographs or diagrams with highlighted areas or notes regarding infrastructure or listing of installation personnel.
3	Persons possessing or observed using night-vision devices near the dam perimeter or in the local area.
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	Personnel being questioned off site about practices pertaining to the dam, or an increase in personal email, telephone calls, faxes, or postal mail concerning the dam or its critical features.
7	Persons not associated with the dam showing an increased general interest in the area surrounding it.
8	Dam personnel willfully associating with suspicious individuals.
9	Computer hackers attempting to access sites looking for personal information, maps, or other targeting examples.
10	An employee who changes working behavior or works more irregular hours.
11	Persons observed or reported to be observing receipts or deliveries, especially of hazardous or toxic materials.
12	Aircraft 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 (ID) cards or uniforms.
15	Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, closed-circuit televisions (CCTVs), intrusion detection systems (IDSs), electric entry control systems, guard dogs, or other security devices.
16	Persons drawing schematics and taking detailed notes of a dam and its associated key features.

Indicators About Activities (Observed or Reported)	
17	Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack-planning activities.
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 (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 the dam's outside components (i.e., an electrical substation not located on site and not as heavily protected or not protected at all).
24	Sudden increases in power outages. Outages could be implemented from an offsite 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), dam safety devices (e.g., piezometers, inclinometers, relief wells) being left unsecured or doors being 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 email 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 heating, ventilating, and air-conditioning (HVAC) equipment or air-intake systems.
36	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
37	Packaging and/or packaging components 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.

Suspicious Activity Indicators

Aggressors may also engage in suspicious activities that could be indicators of a possible threat to a dam. 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-this makes communication between law enforcement agents and owners and operators very important.

Explosives Activities Indicators

- Explosives thefts or sales of large amounts of smokeless powder, blasting caps, or high-velocity explosives.
- Large amounts of high-nitrate fertilizer sales to non-agricultural purchasers or abnormally large amounts to agricultural purchasers.
- Large theft/sales of combinations of ingredients for explosives (e.g., fuel oil, nitrates) beyond normal use.
- Theft/sales of containers (e.g., propane bottles) or vectors (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/sales/reported seizure of night-vision equipment or body armor.

Reporting Incidents

DHS and the Texas Commission on Environmental Quality (TCEQ) joined together to identify what types of surveillance or suspicious incidents should be reported, to whom incidents should be reported, and what information should be conveyed. The following information is from a joint DHS and TCEQ bulletin, Reporting Suspicious Dam Incidents.

Types of Incidents to Report

- Elicitation of inappropriate information
- Breach of a restricted area
- Attempted intrusion into a restricted area
- Photography
- Observation taken to an unusual degree
- Theft
- Sabotage, tampering, or vandalism
- Cyber attack
- Expressed threats
- Flyover
- Weapons discovery

Who Should Receive Incident Reports

DHS encourages recipients of this document to report information concerning suspicious or criminal activity to DHS and/or the FBI. Suspicious activity concerning CIKR should be reported to the National Infrastructure Coordinating Center (NICC), which is the CIKR-focused element of the DHS National Operations Center.

The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov.

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

What Should be Reported

Each incident report should include the following information to the extent possible:

Date and time of incident

Number of individuals involved

Description of the incident

Name and address of the dam

Contact information of the person submitting the report

Suspicious persons

Names, aliases, including variations in spelling

Gender

Physical description

Social Security Number and any passport and visa information

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

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

Boats

Boat 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

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

Complete the agency contact information in the front of this guide.

Build relationships with these agencies before an incident occurs.

Appendix A

Dams Sector Coordinating Council (SCC) Membership

Allegheny Energy

Ameren Services Company

American Electric Power

Association of State Dam Safety Officials

AVISTA Utilities

CMS Energy

Dominion Resources

Duke Energy

Exelon Corporation

National Hydropower Association

National Mining Association (ex officio member)

National Water Resources Association

New York City Department of Environmental Protection

New York Power Authority

Ontario Power Generation

Pacific Gas & Electric Company

PPL Corporation

Public Utility District 1 of Chelan County, WA

Scana Corporation

South Carolina Public Service (Santee-Cooper)

Southern California Edison

Southern Company Generation

TransCanada

U.S. Society on Dams

Xcel Energy Corporation

Appendix B

Dams Sector Government Coordinating Council (GCC) Membership

Department of Agriculture—Natural Resources Conservation Service

Department of Defense—U.S. Army Corps of Engineers

Department of Homeland Security—Office of Infrastructure Protection

Department of the Interior—Bureau of Reclamation

Department of Labor—Mine Safety and Health Administration

Department of State—International Boundary and Water Commission

Federal Energy Regulatory Commission

Tennessee Valley Authority

State governments—Represented by Dam Safety Offices of

California

Colorado

Nebraska

New Jersey

Ohio

Pennsylvania

Virginia

Washington

Appendix C
Acronyms

CCTV	closed-circuit television
CIKR	critical infrastructure and key resources
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FOUO	For Official Use Only
GCC	Government Coordinating Council
HSIN	Homeland Security Information Network
HVAC	heating, ventilating, and air conditioning
ID	identification
IDS	intrusion detection system
JTTF	Joint Terrorism Task Force
NICC	National Infrastructure Coordinating Center
NOC	National Operations Center
SCC	Sector Coordinating Council
SSA	Sector-Specific Agency
TCEQ	Texas Commission on Environmental Quality
WMD	weapons of mass destruction

Appendix D
Bibliography

(Internet sites accessed April/May 2007)

Agricultural, Chemical, and Petroleum Industry Terrorism Handbook, Federal Bureau of Investigation, Department of Justice [http://www.mnhtcia.org/FBIAgChemHandbook.pdf].

"Benefits of Dams," Federal Emergency Management Agency, U.S. Department of Homeland Security [http://www.fema.gov/hazard/damfailure/benefits.shtm].

"Eagle Eyes: Categories of Suspicious Activities" [http://www.osi.andrews.af.mil/eagleeyes/index.asp].

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

National Infrastructure Protection Plan, U.S. Department of Homeland Security, 2006.

"National Inventory of Dams," U.S. Army Corps of Engineers [http://crunch.tec.army.mil/nidpublic/webpages/nid.cfm].

"Potential Indicators of Threats Involving Vehicle-Borne Improvised Explosive Devices (VBIEDs)," U.S. Department of Homeland Security, Information Bulletin, May 15, 2003 [http://www.sanantonio.gov/sapd/pdf/DHS051503.pdf].

"Possible Indicators of Al-Qaeda Surveillance," Department of Homeland Security,

Information Bulletin 03-004, March 20, 2003

[http://www.esisac.com/publicdocs/Other_Advisories/DHS_ib_03-004_aq_survevil.pdf].

"Possible Indicators of Suspicious Activities" [http://www.opr.auxnstaff.org/pdf/handout_susicious.activities.pdf].

"Seven Signs of Terrorist Activity" [http://www.scnus.org/content_display.html?ArticleID=150136].

"Terrorist Attack Indicators" [http://www.ndcap.org/downloads/terrorist_attack_indicators.doc].

"Terrorist Surveillance Indicators" [http://www.scnus.org/content_display.html?ArticleID=151458].

"Terrorist Surveillance Techniques" [http://www.usdoj.gov/usao/wie/atac/publications/Surveillance%20Techniques.pdf].

"Texas Commission on Environmental Quality: Reporting Suspicious Dam Incidents" [http://www.tceq.state.tx.us/assets/public/compliance/field_ops/fod_forms/damsafety/20366.doc]

Developed jointly by:

Dams Sector-Specific Agency

Dams Sector Coordinating Council

Dams Sector Government Coordinating Council

Critical Infrastructure Partnership Advisory Council

Homeland Security