

Dams Sector Security Awareness Guide: Levees

A Guide for Owners and Operators

2008



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 Levee Operator(s) | | |
| Upstream Levee Operator(s) | | |
| | | |
| City Emergency Management | | |
| County Emergency Management | | |
| State Emergency Management | | |
| Federal Emergency Management Agency | | |
| | | |
| U.S. Army Corps of Engineers | | |
| U.S. Coast Guard | | |
| | | |
| Department of Homeland Security (DHS) Protective Security Advisor for the State or Region | | |
| DHS National Infrastructure Coordinating Council (NICC) | nicc@dhs.gov | (202) 282-9201 |
| 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, Association of State Floodplain Managers, AVISTA Utilities, CMS Energy, Dominion Resources, Duke Energy, Exelon Corporation, Hydro-Quebec, National Association of Flood and Stormwater Management Agencies, National Hydropower Association, National Mining Association (ex officio), National Water Resources Association, New York City Department of Environmental Protection (ex officio), New York Power Authority, Ontario Power Generation, Pacific Gas and Electric Company, PPL Corporation, Progress Energy, Public Utility District 1 of Chelan County, WA, Scana Corporation, Seattle City Light, South Carolina Public Service (Santee-Cooper), Southern California Edison(ex officio), Southern Company Generation, U.S. Society on Dams, and Xcel Energy; and the following government security partners: Bonneville Power Administration, 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, Federal Emergency Management Agency, International Boundary Water Commission, Mine Safety and Health Administration, Natural Resources Conservation Service, Tennessee Valley Authority, U.S. Army Corps of Engineers, U.S. Coast Guard, Western Area Power Administration, and state dam safety officials from California, Colorado, Nebraska, New Jersey, Ohio, Pennsylvania, North Carolina, and Washington.

Distribution

This 2008 *Dams Sector Security Awareness Guide: Levees* was prepared under the auspices of the U.S. Department of Homeland Security. For distribution information, contact dams@dhs.gov.

Notice

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

Introduction

The purpose of this guide is to provide information for 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 infrastructure, the technological and national security environment in which the U.S. levee infrastructure is operated and maintained continues to evolve over time. New threats to the continued reliability and integrity of all infrastructure require vigilance. Areas of possible focus by levee 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 is comprised of the assets, systems, networks, and functions related to the Nation's levees, dam projects, navigation locks, hurricane barriers, mine tailings impoundments, or other similar water retention and/or control facilities. 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 and resiliency issues related to 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.

In addition to this guide, the Dams Sector prepared a series of documents that provide more detailed information on security concerns and appropriate responses (*Dams Sector Security Awareness Handbook*), security strategies and protective measures (*Dams Sector Protective Measures Handbook*), and emergency preparedness (*Dams Sector Crisis Management Handbook*).

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

- 1. terrorist surveillance objectives,*
- 2. terrorist surveillance/suspicious activity indicators, and*
- 3. reporting incidents of surveillance/suspicious activity.*

Benefits of Levees to the Nation

Levees are important components of the flood-risk reduction infrastructure systems of many of the Nation's flood-prone communities. The actual number of miles of levees in the United States is unknown but it is estimated at tens of thousands. Additional estimates are that levees protect millions of people. The benefits of levees include:

- Flood-Risk Reduction – By restricting floodwaters, levees reduce loss of life and property damage, and protect critical infrastructure.
- Resource Use – Levees provide flood-risk reduction while allowing agricultural, industrial, commercial, and residential development.
- Navigation – Levees on some river systems facilitate barge traffic by helping to maintain river depths.
- Irrigation – Water sources for some irrigation projects are protected by levees.
- Recreation – Boating, camping, hiking, jogging paths, and picnic areas are supported by levees.

Levees as Critical Infrastructure and Key Resources of the Nation

Critical infrastructure are those assets, systems, and networks, whether physical or virtual, 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 established the Department of Homeland Security (DHS) and defined the protection of the Nation's critical infrastructure and key resources (CIKR) as one of the primary missions of the new department. The act further requires DHS to recommend the measures necessary to protect the country's CIKR but to do so in coordination with other agencies of the Federal Government and in cooperation with State and local agencies and authorities, the private sector, and other entities.

Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, issued in December 2003, builds on the 2002 law. It mandates the development of a National Infrastructure Protection Plan (NIPP) to provide the unifying structure that integrates existing and future CIKR protection efforts into a single national program. The directive also assigns responsibility for CIKR sectors to Federal Sector-Specific Agencies (SSAs). The Office of Infrastructure Protection, a component of the DHS National Protection and Programs Directorate, has been designated as the SSA for the Dams Sector. The SSA is responsible for implementing the risk management framework and sector partnership model described in the NIPP.

The Dams Sector partners include the Federal, State, regional, local, tribal, and territorial government entities that own, operate, or regulate levees; private sector levee owners and operators; and organizations that share in the responsibility for protecting levees. The cooperation needed among DHS

and the Dams Sector partners to provide this protection is accomplished through the collaborative framework embodied in the NIPP and implemented through the formation of coordinating councils.

The Dams Sector Coordinating Council (SCC) is self-organized, self-run, and self-governed. It is the primary interface with DHS for private and State and local government owners and operators of dams, locks and levees on security issues. Its members are representative of the range of assets within the sector. The SCC helps determine the nature of risks posed against sector infrastructure so that appropriate and timely information, as well as mitigation strategies, can be provided to the entities responsible for the operation and protection of those assets. The membership of the SCC is provided in Appendix A.

The Levee Sub-Sector Coordinating Council was formed in 2008 as an adjunct to the Dams SCC. Its membership includes representatives from the National Association of Flood and Stormwater Management Agencies (NAFSMA) and the Association of State Floodplain Managers (ASFPM) as well as individual levee owners and operators. The levee representatives also participate in overall Dams Sector activities; the Sub-Sector Coordinating Council chairman and vice-chairman serve as voting members of the Dams SCC.

The Dams Sector Government Coordinating Council (GCC) acts as the counterpart and partner to the SCC to plan, implement, and execute sector-wide CIKR protection programs for the sector's assets. It is comprised of Federal agency owners and operators and State and Federal regulators of sector assets. It enables public-private coordination and communication and brings together diverse Federal and State interests. GCC membership is provided 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, comprised of representatives of the SCC, GCC, and SSA, initiated development of the guide. The workgroup recognized that levees 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.

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 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 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. After surveillance of a target has concluded and preparations for the attack are complete, a final pre-operational survey 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 or walking by a site to observe the facility or site operations and is the most probable technique to observe and assess levees during the initial phases of a surveillance effort. 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 or persons walking on or around the levee for reasons that do not seem obvious.

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 levee, over an extended period of time. They may also pose as fishermen, farm workers, recreational users, tourists, or photographers 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 a levee may be under surveillance are those warning signs that the normal environment isn't quite what it should be—that seemingly normal activities seem some-

what suspicious. The following table of possible indicators of surveillance activity points out some of those warning signs.

Table 1: Indicators of Possible Surveillance

| Indicators About Activities (Observed or Reported) | |
|---|---|
| 1 | Persons using or carrying video/camera/observation equipment. |
| 2 | Persons with installation maps or photos 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 levee 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 levee or an increase in personal e-mail, telephone, faxes, or postal mail concerning the levee or its critical features. |
| 7 | Persons not associated with the levee showing an increased general interest in the area surrounding it. |
| 8 | Levee 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 | A noted pattern or series of false alarms requiring a response by law enforcement or emergency services. |
| 12 | Theft of contractor identification cards or uniforms or unauthorized persons in possession of identification (ID) cards or uniforms. |
| 13 | 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. |
| 14 | Persons drawing schematics and taking detailed notes of a levee and its associated key features. |

Indicators About Activities (Observed or Reported)

| | |
|----|---|
| 15 | Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack-planning activities. |
| 16 | Repeated attempts from the same location or country to access protected computer information systems. |
| 17 | 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. |
| 18 | Attempts to obtain information about the levee (e.g., blueprints of buildings, security measures or personnel, entry points, access controls, or information from public sources). |
| 19 | Unfamiliar contract workers with passable credentials; crews or contract workers attempting to access unauthorized areas. |
| 20 | A seemingly abandoned or illegally parked vehicle in the area of the levee. |
| 21 | Increase in buildings, fence gates, controls, safety devices (e.g., piezometers, inclinometers) being left unsecured or doors being left unlocked that are normally locked at all times. |
| 22 | 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. |
| 23 | Increase in violation of security guard standard operating procedures for staffing key posts. |
| 24 | Increase in threats from unidentified sources by telephone, by postal mail, or through the e-mail system. |
| 25 | Increase in reports of threats from outside known, reliable sources. |
| 26 | Sudden losses or theft of operations communications equipment. |
| 27 | Displaced or misaligned manhole covers or other service access doors on or surrounding the asset site. |
| 28 | Unusual maintenance activities (e.g., road repairs) near the asset. |
| 29 | Observations of unauthorized personnel collecting or searching through trash. |
| 30 | Unusual packages or containers, especially near pumping stations or gates. |
| 31 | Unusual powders, droplets, or mist clouds near pumping stations or gates. |

Suspicious Activity Indicators

Aggressors may also engage in suspicious activities that could be indicators of a possible threat to a levee. The suspicious activity indicators listed below are more likely to be known or observed by local law enforcement agencies than by levee owners and operators—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 or 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.

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.

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, especially concerning mechanical components of the levee system such as pumping stations and gates.
- Theft.
- Sabotage, tampering, or vandalism.
- Cyber attack.
- Expressed threats.
- Flyover.
- Weapons discovery.

Who Should Receive Incident Reports

Local law enforcement should be notified of suspicious incidents. DHS encourages recipients of this document to also report information concerning suspicious or criminal activity to DHS and/or the FBI. This reporting should be done according to the protocols established by the levee owner or operator.

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 <http://www.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, with an identifier of the levee involved

Name and address of the levee owner/operator

Contact information of the person submitting the report

Suspicious persons

Names, aliases (including variations in spelling)

Gender

Physical description

Social Security Number, driver's license, 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 similar incidents involving the 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

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

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 and Levee Sub-Sector Coordinating Council Membership

The Dams Sector Coordinating Council and Levee Sub-Sector Coordinating Council are self-organized, self-run, and self-governed organizations that represent the spectrum of assets within the Dams Sector. The councils are the government's principal point of entry into the sector for developing and coordinating CIKR protection activities and issues. Membership in the councils is as follows.

Dams Sector Coordinating Council (SCC) Membership

Allegheny Energy
Ameren Services Company
American Electric Power
Association of State Dam Safety Officials
Association of State Floodplain Managers
AVISTA Utilities
CMS Energy
Dominion Resources
Duke Energy
Exelon Corporation
Hydro-Quebec
National Association of Flood and Stormwater Management Agencies
National Hydropower Association
National Mining Association (ex-officio member)
National Water Resources Association

New York City Department of Environmental Protection (ex-officio member)
New York Power Authority
Ontario Power Generation
Pacific Gas & Electric Company
PPL Corporation
Progress Energy
Public Utility District 1 of Chelan County, WA
Scana Corporation
Seattle City Light
South Carolina Public Service (Santee-Cooper)
Southern California Edison (ex-officio member)
Southern Company Generation
U.S. Society on Dams
Xcel Energy Corporation

Levee Sub-Sector Coordinating Council Membership

National Association of Flood and Stormwater Management Agencies
Association of State Floodplain Managers
Los Angeles County Flood Control District
Reclamation District 1000 (Natomas, CA)
South Lafourche Levee District

Appendix B

Dams Sector Government Coordinating Council (GCC) Membership

The Dams Sector Government Coordinating Council is the government counterpart to the SCC. It is comprised of Federal agency owners and operators of sector assets and State and Federal regulators of sector assets. The composition of the council enables communication and coordination among agencies. Members of the GCC are as follows.

Bonneville Power Administration

Department of Agriculture—Natural Resources Conservation Service

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

Department of Homeland Security—Office of Infrastructure Protection; Federal Emergency Management Agency; U.S. Coast Guard.

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

Western Area Power Administration

State governments—Represented by Dam Safety Offices of

California

Colorado

Nebraska

New Jersey

Ohio

Pennsylvania

North Carolina

Washington

Appendix C

Acronyms

| | | | |
|-------|--|--------|--|
| ASFPM | Association of State Floodplain Managers | JTTF | Joint Terrorism Task Force |
| CCTV | closed-circuit television | KR | key resource |
| CI | critical infrastructure | NAFSMA | National Association of Flood and Stormwater Management Agencies |
| DHS | Department of Homeland Security | NICC | National Infrastructure Coordinating Center |
| FBI | Federal Bureau of Investigation | NIPP | National Infrastructure Protection Plan |
| GCC | Government Coordinating Council | SCC | Sector Coordinating Council |
| HSPD | Homeland Security Presidential Directive | SSA | Sector-Specific Agency |
| ID | identification | TCEQ | Texas Commission on Environmental Quality |
| IDS | intrusion detection system | WMD | weapons of mass destruction |

Appendix D

References

(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]

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

Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection* [http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf]

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

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

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]

“Terrorist Threats Reporting Guide” [www.tisp.org/files/pdf/ci_jan_07_2005.pdf]

“Texas Commission on Environmental Quality: Reporting Suspicious Dam Incidents” [http://www.tceq.state.tx.us/assets/public/compliance/field_ops/fod_forms/dam-safety/20366.doc]

Developed jointly by:

Dams Sector-Specific Agency

Dams Sector Coordinating Council

Levee Sub-Sector Coordinating Council

Dams Sector Government Coordinating Council

Critical Infrastructure Partnership Advisory Council



Homeland
Security