Dams Sector Security Awareness Handbook

A Guide for Owners and Operators

2007

Homeland Security

For Official Use Only (FOUO)

List response agencies for your community and geographic region. Build relationships with these groups before an incident occurs.

Resource	Contact	Telephone 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 Advisor 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 of 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 & 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; United States Society on Dams; and Xcel Energy, and the following government security partners: Bureau of Reclamation (which also serves as the 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.

The Dams Sector would also like to thank and acknowledge information contributions from the Federal Bureau of Investigation, the North American Electric Reliability Council, and Argonne National Laboratory.

Distribution

This 2007 *Dams Sector Security Awareness Handbook* was prepared under the auspices of the U.S. Department of Homeland Security. Two additional handbooks are in development: *Dams Sector Protective Measures Handbook* and *Dams Sector Crisis Management Handbook*. These materials will be available on the Homeland Security Information Network (HSIN). For additional distribution information, contact dams@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.

Table of Contents

List of Figures

List of Tables

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 infrastructure requires 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 is comprised of 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, Territorial, regional, 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 Nation has more than 100,000 dams. Of this number, approximately 82,000 are listed in the National Inventory of Dams (NID), which generally includes dams greater than 25 feet in height or reservoirs having more than 50 acre-feet in storage capacity. In the NID, the downstream hazard potential (e.g., the amount of risk or damage a dam can pose because of failure or negligent operation) is classified as high, significant, or low. In the current NID database, approximately 12,000 dams are classified as high hazard potential from a dam safety perspective. However, only a very small percentage of high-hazard dams represent a potential for causing mass casualties.

Dams are a vital part of the Nation's infrastructure and are among its key resources. Dams provide a range of economic, environmental, and social benefits, including irrigation, electric power generation, "black start" capabilities, water storage, recreation, navigation, flood mitigation, sediment/hazardous materials (HAZMAT) control, and mine tailings impoundment.

Target Audience

This handbook has been prepared for owners and operators of dams, regardless of facility size or type.

The benefits of dams, however, are countered by the risks that they present. In the event of a dam failure, the potential energy of the water stored, even behind a small dam, is capable of causing loss of life and significant property damage.

Dams may fail for one or a combination of the following reasons:

- Overtopping;
- Structural failure;
- Foundation failure;
- Piping and internal erosion;
- Inadequate maintenance;
- Operational errors; and/or
- Deliberate manmade actions.

The dams industry has a long history of recognizing and dealing with these potential issues. However, deliberate, manmade actions are an area of more recent concern. This Security Awareness Handbook is designed to assist owners and operators in dealing with that issue by reinforcing good security practices. While the average dam owner or operator does not need to be a "security expert," security awareness is the foundation upon which effective security programs are based.

Purpose

- The *Dams Sector Security Awareness Handbook* focuses attention on security issues related to dam infrastructures by providing information for owners and operators that allows them to recognize security concerns and respond accordingly.
- Owners and operators are encouraged to reach out to, establish partnerships with, and share information with law enforcement, emergency management, and emergency responders before an incident occurs.

This handbook is organized into four sections and includes related appendixes. Section 1 contains an overview of the Dams Sector, its regulatory structure, characteristics, the possible effects of dam failure, and the organizations and agencies involved in dam safety and security. Section 2 presents information about security-related vulnerabilities that are common to the Dams Sector, based on security assessments that have been performed on Dams Sector assets. Section 3 introduces information about indicators that suggest that criminal or terrorist activity may be taking place. Section 4 contains guidelines for reporting suspicious activities and incidents, recognizing, however, that specific reporting procedures may already exist in your region, State, community, or organization and should be followed first and foremost.

Key definitions and information on Federal initiatives that support Dams Sector security are provided in appendixes A and B, respectively. Appendixes C and D describe executive orders, presidential decision directives, homeland security presidential directives, and laws applicable to the Dams Sector. Members of the Dams Sector Coordinating Council (SCC) and the Dams Sector Government Coordinating Council (GCC) are listed in appendixes E and F, respectively. The acronyms and abbreviations used in the handbook are listed and defined in appendix G, and appendix H lists reference materials of interest to Dams Sector security partners.

The Homeland Security Act of 2002, Homeland Security Presidential Directive 7 (HSPD 7), as well as other Federal initiatives, resulted in the establishment of the Department of Homeland Security (DHS) and identified dams as one of 17 critical infrastructure and key resources (CIKR) sectors. CIKR sectors include electricity, water, nuclear, communications, and others. The DHS has been identified as the Sector-Specific Agency for the Dams Sector. The DHS is responsible for the issuance of a National Infrastructure Protection Plan (NIPP) that outlines its strategy for protecting the national infrastructure. Each sector also develops a plan specific to the needs of the individual sector. To coordinate those strategies, each sector, including dams, has established a Government Coordinating Council and a Sector Coordinating Council broadly representing the private sector. The Dams Sector councils were formed in 2005 and meet separately and jointly on a quarterly basis.

The Dams Sector completed a Dams Sector-Specific Plan at the end of 2006 that serves as a vehicle for the sector security partners to work cooperatively with the DHS to identify issues, set goals, create strategies, and implement protective programs that make effective use of available resources. The sector security partners have jointly identified security-related priorities for the Dams Sector, which include, among other items, the need for developing mechanisms for the communication of security issues among member organizations. This handbook is one outcome of that process and was developed by the Dams Sector Security Education Workgroup, which is composed of members of both the Dams Sector GCC and SCC.

Further information about the NIPP and a listing of the 17 CIKR sectors is provided in appendix B of this handbook. Additional information about the NIPP is also available on the Internet at www.dhs.gov/nipp.

For additional information, also see:

Dams Sector Protective Measures Handbook
An overview of measures to detect, deter, and defend assets.
Dams Sector Crisis Management Handbook
An overview of of preparedness and response suggestions.

Section 1: Sector Overview

Regulatory Structure

The regulatory structure for sector assets in the United States is divided between the Federal Government and the States.

Dams owned by Federal agencies are self-regulated. The States regulate most of the non-Federal dams that are not regulated by the Federal Energy Regulatory Commission (FERC). In addition, most hydroelectric facilities are subject to regulation by FERC, which includes approximately 2,600 facilities.

Nearly all States have dam safety regulatory programs. State governments have regulatory responsibility for 86 percent of the approximately 82,000 dams within the National Inventory of Dams (NID). These programs vary in authority. Most States have legislative authority to carry out a comprehensive dam safety program. Some States are unable, by specific language in their laws, to regulate certain types of dams. Many States have limited resources to enforce the law.

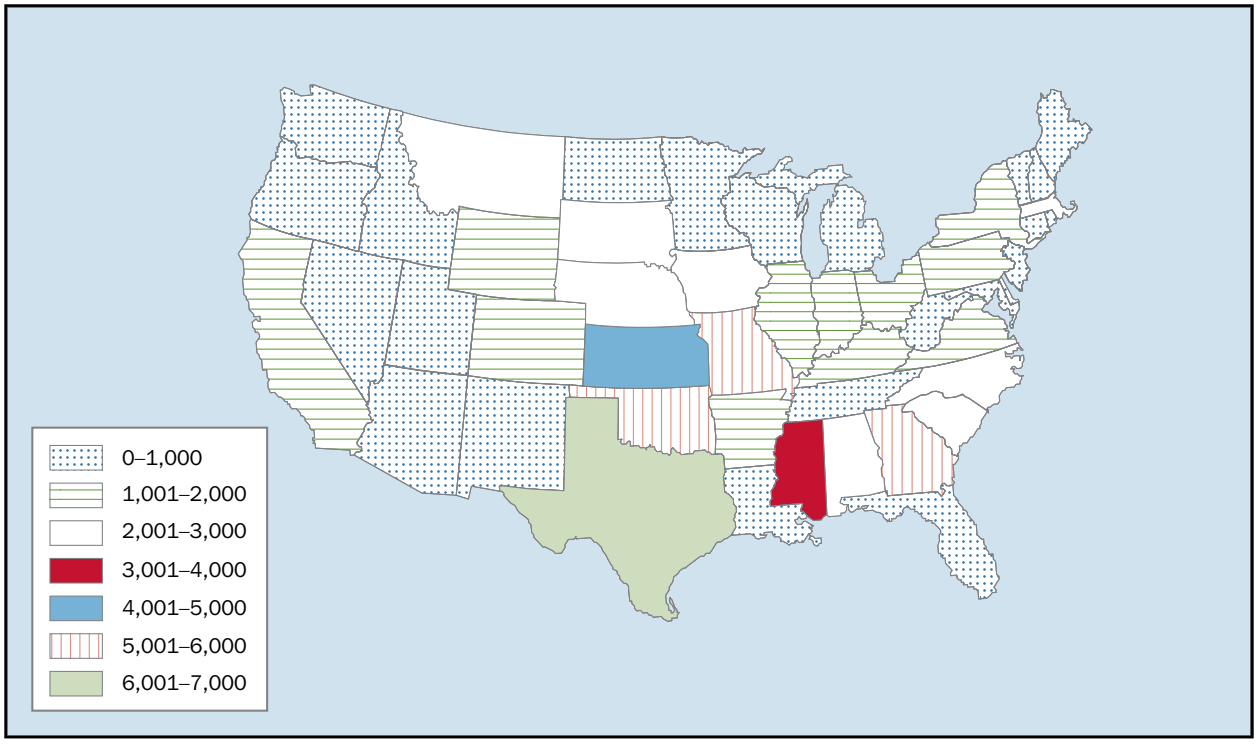
Although, presently, there is no nationwide authority governing levees, efforts are underway to establish a levee safety program. For levees that are owned and operated by the U.S. Army Corps of Engineers (USACE), operation and maintenance are managed through the operation and maintenance budget process. For levees built by USACE and operated and maintained by a local sponsor, USACE's only authority is to inspect sponsors for compliance. Some State governments have initiated various activities to regulate and/or inventory levees within their State boundaries.

Mine tailings impoundments are generally subject to the Federal Mine Safety and Health Act (MSHA), which regulates to protect the health and safety of miners, and the Surface Mining Control and Reclamation Act (SMCRA), which regulates to protect society and the environment from the adverse effects of surface mining operations. The MSHA regulates impoundments of water, sediment, or slurry with an elevation of 5 feet or greater that have a storage volume of 20 acre-feet or more, or impound to an elevation of 20 feet or greater, or present a hazard to miners. The SMCRA specifies that because of diversity in terrain, climate, biology, geochemistry, and other physical conditions under which mining operations occur, the primary government responsibility for regulating surface mining and reclamation operations should rest with the States. To achieve primary regulatory responsibility, often referred to as primacy, a State must develop a program that demonstrates the State's capability to carry out the relevant provisions of the SMCRA. Currently, 24 States have primacy; 12 do not. Mine tailings impoundments, like conventional dams, may also be subject to other Federal and State statutes that relate to impoundments, such as the Clean Water Act, the Clean Air Act, the Safe Drinking Water Act, the Resource Conservation and Recovery Act, and others.

Number and Distribution of Dams

The NID, which is maintained by the USACE, lists approximately 82,000 dams. In general, to be listed in the NID, a dam must be more than 25 feet in height or have more than 50 acre-feet in reservoir storage. The NID also includes some smaller structures that pose a safety hazard to the downstream population. The total number of dams in the Nation, including non-NID-listed dams, is estimated at 100,000. Figure 1-1 shows the distribution of dams in the contiguous United States.

Figure 1-1: Distribution of Dams in the Contiguous United States



The largest dams reach almost 800 feet in height or 28 million acre-feet of storage capacity. The smallest dams are only several feet high or have just a few acre-feet of storage. Dams are widely distributed in every State in the country.

Most dams in the United States are privately owned (approximately 65 percent). Local governments own and operate the next largest number of dams (approximately 20 percent), followed by State ownership (approximately 5 percent). The Federal Government, public utilities, and undetermined interests account for the remaining 10 percent. However, many of the largest, most famous dams are federally owned.

Purpose of Dams

Dams impound water or water-borne materials for several reasons: flood control/flood damage reduction (hereafter, flood control), human and livestock water supplies, irrigation, energy generation, containment of mine tailings, recreation, and debris control (many dams fulfill a combination of these functions). For example, 10 percent of American cropland is irrigated by using water stored behind dams. The NID lists the primary purposes for dams in the Nation as follows:

Recreation	34.4%
Flood Control	16.6%
Fire Protection, Stock, or Small Farm Pond	14.7%
Irrigation	10.1%
Water Supply	7.2%
Other [1]	6.7%
Unknown [2]	3.8%
Hydroelectric	2.5%
Fish and Wildlife Pond	2.1%
Tailings	1.1%
Debris Control	0.5%

[1]Dams that do not fit into any of the listed categories.

[2]Purpose was not entered into the NID.

Common Characteristics of Dams

The purpose of dams is to help harness and manage the Nation's water resources. Dams retain water, but also provide a means to release water in a controlled manner.

Dams consist of multiple component structures, depending on the purpose of the project. Typical components include embankments, concrete gravity sections, gated spillways, ungated or auxiliary spillways, navigation locks, hydropower houses, control towers, conduits and tunnels, relief wells, galleries, holes for instrumentation to monitor water pressure on and within the structures, drains, seepage barriers such as upstream blankets, or grout curtains. Figure 1-2 illustrates some components of a dam, and figure 1-3 shows some water control gates that are used at dams.

Figure 1-2: Example Components of a Dam

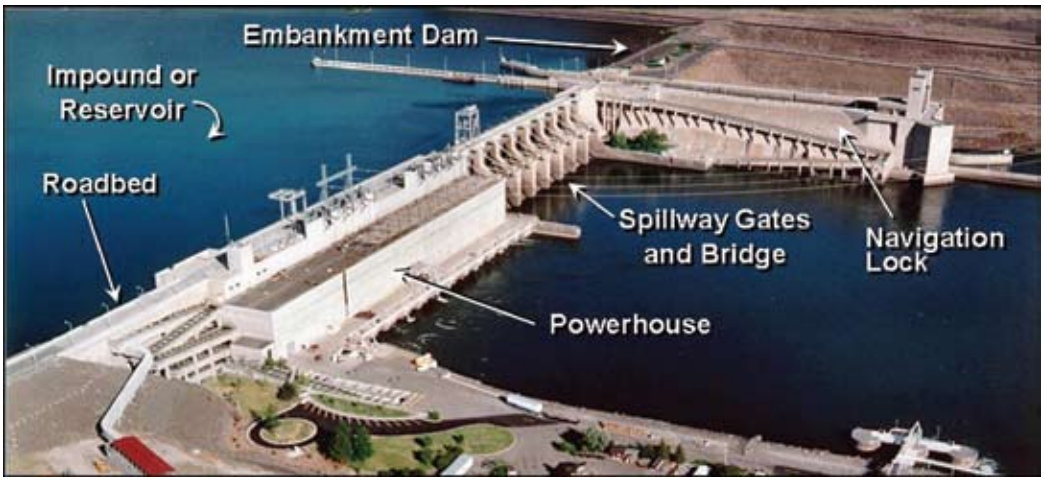
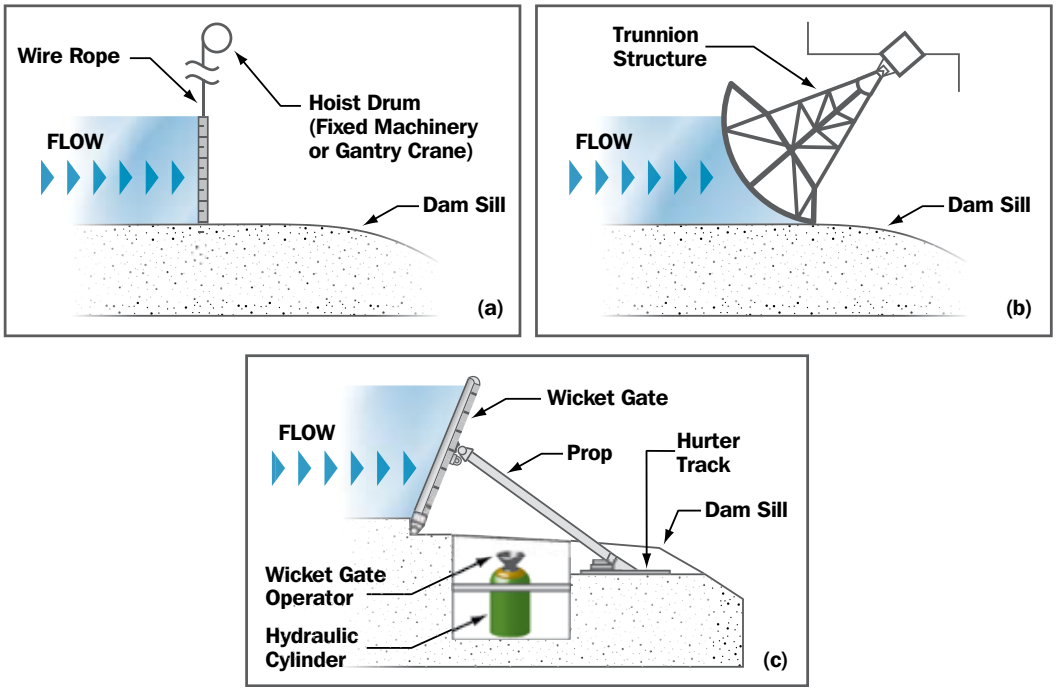


Figure 1-3: Types of Gates: (a) Vertical Lift, (b) Tainter, and (c) Wicket



Dams are constructed in various ways. Embankment dam sections may be hydraulic fill, homogeneous, or zoned earth and/or rock fill. Concrete dam sections may be gravity sections, arch, or a combination gravity-arch structure. Concrete-faced, rock-fill dams are also common in the United States.

Because a major role of a dam is to retain water effectively and safely, the water-retention ability of a dam is of prime importance. Water can pass from the reservoir to the downstream side of a dam by:

- Passing through the main spillway or outlet works;
- Passing over an auxiliary spillway;
- Overtopping the dam; or
- Seeping through abutments or under the dam.

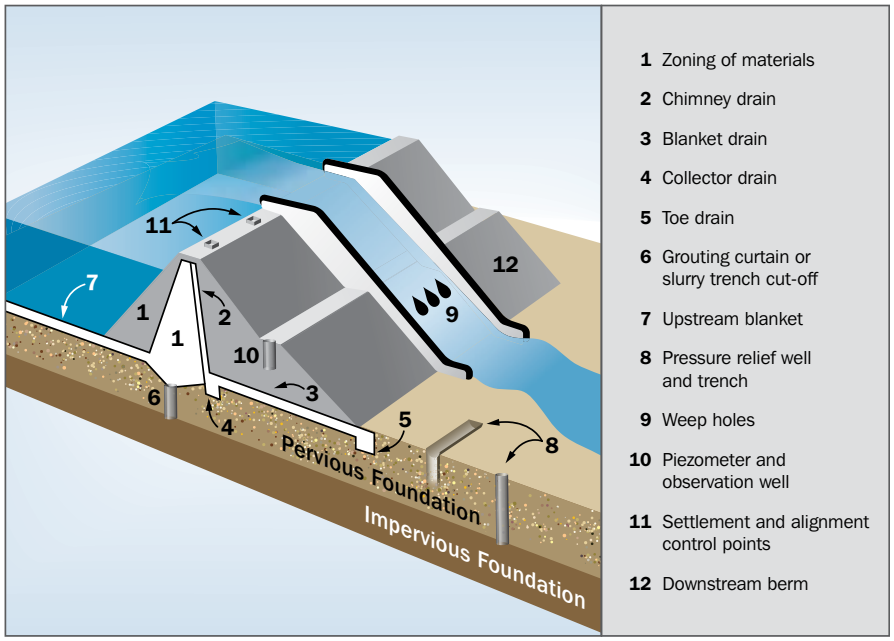
Water normally passes through the main spillway or outlet works. Generally, water passes over an auxiliary spillway only during periods of high reservoir levels. Spillway features are also used to lower reservoir levels for repair and safety concerns. Overtopping of an earth-fill embankment dam is undesirable because the embankment materials may be eroded away.

All embankment and most concrete dams have some seepage. However, it is important to control the seepage to prevent internal erosion and instability. Proper dam construction, maintenance, and monitoring of seepage provide this control. Figure 1-4 illustrates various seepage control strategies.

The retention of the reservoir is a key mission of essentially every dam. A failure of the dam (or associated structures) that allows an uncontrolled release of water is likely to lead to property damage and the potential loss of life to downstream areas if the dam is a high or significant hazard-potential dam. Note, however, that the loss of the reservoir does not necessarily result from a catastrophic failure of the dam; it can also occur because of the failure of discrete project features, such as spillway gates and valves that release water on a much smaller scale.

Physical failure of the dam or its associated structures is a key consideration. In some cases, however, failure of components could potentially result from manipulation or failure of the Supervisory Control and Data Acquisition (SCADA) system, which, if present at a facility, controls and operates gates and valves, allowing more water than desired to exit the reservoir.

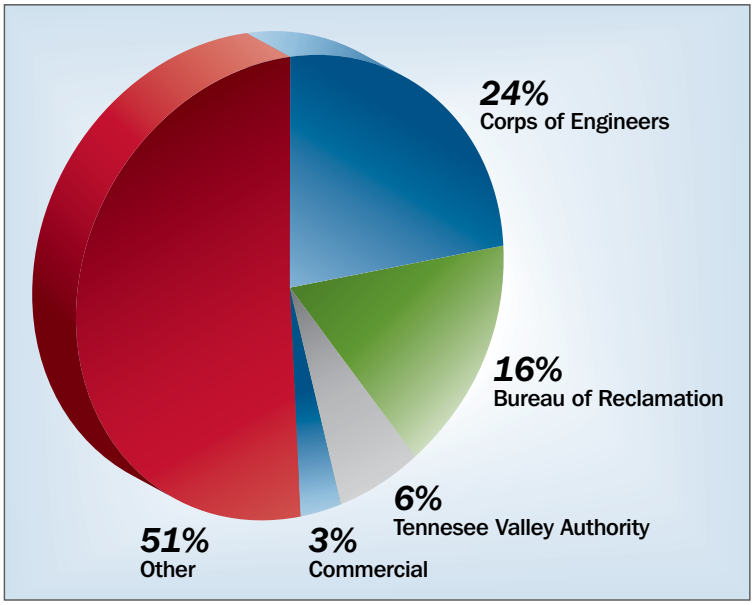
Figure 1-4: Various Seepage Control Strategies



Hydroelectric Plants

Hydropower, including pumped storage, constitutes approximately 8 percent of the electrical generating capacity of the United States. Hydropower is the Nation's primary source of renewable energy. Total U.S. hydroelectric capacity is 103.8 gigawatts (GW), including pumped storage projects. The Federal Government owns 38.2 GW at 165 sites (excluding pumped storage). Another 40 GW of non-Federal, licensed conventional hydroelectric capacity (excluding pumped storage) exists at 2,162 sites around the country according to the National Hydropower Association. Figure 1-5 shows the distribution of hydroelectric generating capacity in the United States.

Figure 1-5: Distribution of Hydroelectric Generating Capacity



Federal ownership of hydroelectric facilities is concentrated in the USACE, the Bureau of Reclamation (Reclamation), and the Tennessee Valley Authority (TVA).

The USACE is the largest hydropower producer, with 350 generating units and a total rated capacity of 21 GW. Most of the USACE hydropower capacity is concentrated in the Northwestern Division, which, according to the USACE, includes 14 dams with more than 100 megawatts (MW) of rated capacity.

Reclamation has less hydropower capacity than the USACE, with a total of 14.8 GW produced at 58 hydroelectric plants. The bulk of Reclamation's hydroelectric capacity, however, is concentrated in a few large dams in the Western United States.

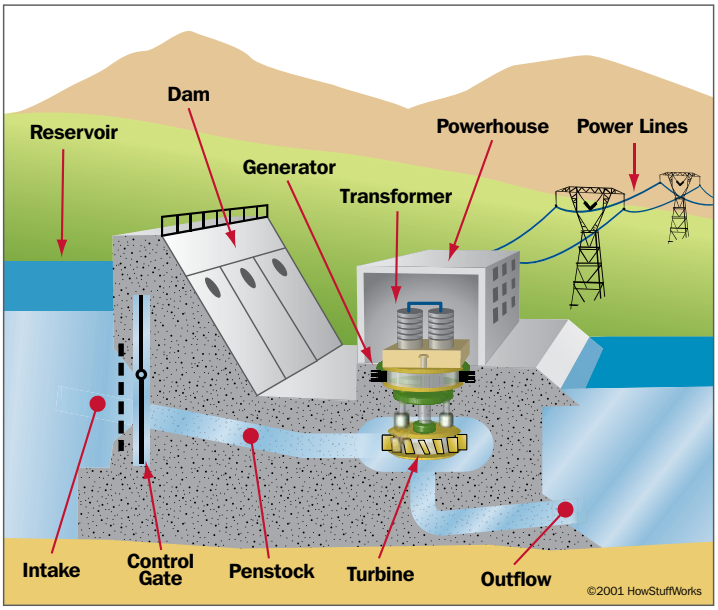
The TVA maintains 29 conventional hydroelectric dams throughout the Tennessee River system and 1 pumped-storage facility for the production of electricity. TVA hydroelectric facilities have a total capacity of approximately 5 GW. Altogether, TVA operates 15 dams with more than 100 MW of hydroelectric generating capacity. In addition, four commercially operated dams on the Little Tennessee River and eight USACE dams on the Cumberland River contribute to the TVA power system.

Most non-Federal hydroelectric dams are operated by power companies and are licensed by FERC. In 2001, FERC regulated 2,600 facilities.

Actual generation supplied by hydropower facilities varies from year to year, depending on rainfall and other factors. For example, in 1999, hydropower supplied 8.5 percent of the electricity generated in the United States. In some States, however, the percentage is much higher, primarily in the West.

Figure 1-6 illustrates various components of a Hydroelectric Dam.

Figure 1-6: Features of a Hydroelectric Dam



Consequences of a Dam Failure

As is the case in any dam failure, the consequences of a deliberate attack on a dam can be wide-ranging and depend heavily on a number of variables: the type of dam itself, what lies downstream, the nature of the failure, and the state of reservoirs above and below the dam. Table 1-1 lists some of the consequences that could result from dam failure and sudden flooding.

Table 1-1: Consequences Related to Failure of a Dam

Human Impact (Public Health and Safety) • Direct loss of life • Flood-caused pollution (e.g., if impounding untreated industrial waste) • Damage to downstream water treatment facilities • Loss of domestic water supply
Economic Impact • Property damage • Loss of project-specific benefits (e.g., power generation, flood control, irrigation, navigation, recreation) • Loss of area business (e.g., products, services, payroll) • Emergency response and cleanup costs
Impact on Public Confidence • Displacement of downstream persons/communities • Damage to infrastructure (e.g., roads, communications, pipelines) • Loss of local/State tax revenue because of property damage • Loss of confidence and other psychological impacts
Impact on Government Capability (National Security and Government Functionality) • Damage to downstream military or law enforcement facilities or to infrastructures serving those facilities (e.g., electrical system or water supply)
Other Impact • Compromise of the mission of downstream dams and upstream reservoirs

One of the most famous dam failures in American history was the Teton Dam break in 1976 (see figure 1-7). Teton Dam, a Reclamation dam in Idaho, failed for reasons that were never fully characterized. It was a just-completed earthfill dam approximately 3,000 feet wide and 300 feet high. Teton Reservoir, formed by the construction of Teton Dam, was to provide a supplemental water supply to 111,210 acres of land in the Fremont-Madison Irrigation District, local and downstream flood control benefits, water to operate a 16,000-kilowatt power plant, and major recreation developments. It was a medium-size dam in comparison to other Reclamation projects. Teton Dam failed on June 5, 1976, when the reservoir, still filling, was within 20 feet of its design depth. Floodwaters coursed down the Teton River and into the Snake River; the flood was finally contained at the American Falls Reservoir approximately 70 miles downstream.

Nine lives were lost and 4,095 homes were destroyed, along with 4,073 farm buildings. Other damage included 100,000 acres of farmland inundated, 427,000 acres of land left without irrigation, 252 businesses interrupted, 21 miles of railroad and 120 miles of vehicular road disrupted, and 250 miles of power lines damaged or destroyed.

Figure 1-7: Failure of the Teton Dam

An example of the consequences of a successful attack on a dam is the willful destruction of the Mohne and Eder dams in Germany during World War II. Both dams were successfully bombed by the English in a deliberate attempt to cause their failure. The resulting impacts from the failure of the Mohne Dam, which involved the release of 116 million cubic meters of water within 12 hours, included the destruction of 92 homes and 11 factories and damage to 2 Mohne power stations, 971 homes, 32 farms, and 50 road or rail bridges. The number of dead or missing people was placed at 1,294. More than 35 percent of the region's industrial production was lost as a result of the destruction of both dams and regional water production dropped by 75 percent.

Dams Sector Security Partners

Many organizations enable Dams Sector security partners to design, finance, construct, operate, regulate, and protect their infrastructures. The coordinating councils for the Dams Sector are the primary mechanism used by DHS to establish and enhance relationships among all sector security partners. Dams Sector security partners are described in the sections below.

Department of Homeland Security

The authority for the DHS's involvement in the Dams Sector is derived from the Homeland Security Act of 2002. The DHS provides a unifying core for the national network of organizations and institutions involved in efforts to secure the Nation's CIKR, which includes dams.

Sector-Specific Agency

The Office of Infrastructure Protection within the DHS has been designated as the Sector-Specific Agency (SSA) for the Dams Sector.

Owners and Operators of Private Dams

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

Other Federal Departments and Agencies

The Dams Sector Government Coordinating Council (GCC) is the primary interface with the DHS for dams that are not privately owned. The GCC membership is listed in appendix F.

The following Federal departments and agencies have important roles in the Dams Sector as owners, operators, or regulators of sector assets:

- **U.S. Department of Agriculture (USDA).** USDA is a major planner, designer, financier, constructor, owner, and/or regulator of more than one-third of all dams in the United States that are included in the NID. A major component within USDA is the Natural Resources Conservation Service, which designs, finances, and constructs dams under its technical and financial assistance programs for individuals, groups, organizations, and governmental units for the purposes of water storage, sediment detention, and flood protection.
- **U.S. Army Corps of Engineers (USACE).** As an element of the Department of Defense (DOD), USACE has responsibility or jurisdiction for: (1) dams that it plans, designs, constructs, and operates; (2) dams that it designs and constructs, but are operated and maintained by others; (3) non-USACE dams and reservoir projects subject to section 7 of the Flood Control Act, the Federal Power Act, as amended, and other laws for which USACE is responsible for prescribing regulations for the use of storage allocated to flood control and/or navigation; (4) dams for which USACE issues permits under its regulatory authority; and (5) dams that USACE inventoried and inspected under the National Dam Inspection Act of 1972, the Dam Safety Act of 1986, and the National Dam Safety Program Act of 1996.
- **U.S. Department of the Interior (DOI).** As the Nation's principal conservation agency, DOI is responsible for most of the U.S. owned public lands and natural resources. DOI is responsible, through its bureaus, for the planning, design, construction, operation, and maintenance of nearly 2,000 dams.
  - The Bureau of Reclamation is a Federal water resource management and development bureau authorized to operate in 17 Western States. In carrying out its mission, Reclamation develops water resource projects where dams play a major role in the viable development of the resources.
  - The Bureau of Indian Affairs (BIA) works with American Indian Tribes to operate and maintain dams on Indian reservations.
  - The Bureau of Land Management is responsible for agency-owned dams on public lands in 11 Western States, including Alaska.
  - The U.S. Fish and Wildlife Service operates facilities associated with fish and wildlife conservation on national wildlife refuges, waterfowl production areas, and national fish hatcheries.
  - The National Park Service (NPS) manages streamflow control structures and monitors the status of non-NPS structures that are within or adjacent to park boundaries.
  - The Office of Surface Mining (OSM) regulates surface coal mining operations and the surface effects of underground coal mining operations. OSM regulates structures through the Western Regional Coordinating Center in Denver, CO, and the Knoxville Field Office in Tennessee.
- **U.S. Department of Labor (DOL).** DOL has Dams Sector responsibilities under the Federal Mine Safety and Health Act for dams constructed by the mining industry. The act specifically includes "impoundments, retention dams, and tailing ponds" as part of a "coal or other mine."
- **International Boundary Water Commission (IBWC), United States, and Mexico.** IBWC has jurisdiction over two large international storage dams and four small diversion dams on the Colorado River and the Rio Grande. The U.S. section of the IBWC is also responsible for maintaining several other dams and river control structures that are not fully international in nature.
- **Federal Energy Regulatory Commission (FERC).** FERC is authorized by the Federal Power Act, as amended, to issue licenses to individuals, corporations, States, and municipalities to construct, operate, and maintain dams, water conduits, reservoirs, powerhouses, transmission lines, or other project works necessary for the development of non-Federal hydroelectric projects on: (1) navigable streams, (2) the public lands of the United States, (3) streams over which Congress has jurisdiction under the Commerce Clause of the U.S. Constitution, and (4) at any Federal Government dam.

- **Tennessee Valley Authority (TVA).** TVA is authorized by the Tennessee Valley Authority Act to approve plans for the construction, operation, and maintenance of all structures affecting navigation, flood control, or public lands or reservations in the Tennessee River System.

State Agencies

State governments have primary responsibility for protecting their populations from dam failure; they have regulatory responsibility for approximately 86 percent of the dams listed in the NID. Although programs vary in the scope of their authority from State to State, program activities typically provide for: (1) safety evaluations of existing dams, (2) reviews of plans and specifications for dam construction and major repairs, (3) periodic inspections of construction of new dams or at existing dams, and (4) review and approval of emergency action plans (EAPs).

The Dam Safety and Security Act of 2002 provides assistance to enhance State programs through grants and technical research and training. Funds provided annually through grants to State dam safety programs can be used by the States to develop dam security vulnerability screening tools and threat response plans for dams with high hazard potential. State assistance under the National Dam Safety Program is intended to help States bring the necessary resources to bear on inspection, classification, and emergency planning for dam safety.

Sector-Related Organizations

A number of existing organizations have a significant influence on the Dams Sector:

- The National Dam Safety Review Board (NDSRB) monitors the safety of dams in the United States and State implementation of dam safety activities, and advises the Federal Emergency Management Agency (FEMA) on national dam safety policy.
- The Interagency Committee on Dam Safety (ICODS) was formally established by the National Dam Safety Program Act in 1996 and is chaired by FEMA. Its main goal is to encourage the establishment and maintenance of effective Federal programs, policies, and guidelines intended to enhance dam safety through coordination and information exchange among Federal agencies. ICODS issued the *Federal Guidelines for Dam Safety*.
- Created in 1997, the Interagency Forum on Infrastructure Protection (IFIP) is a consortium of U.S. Government agencies that represent power dam owners, transmission system operators, and anti-terrorism/security experts. IFIP partners developed the Incident Reporting System Program, under the auspices of the USACE Intelligence and Security Countermeasures Branch, to share threat, warning, and point analysis. They also developed the first comprehensive risk assessment methodology designed specifically for dams and electric power transmission systems.

Relationships With Tribal Government Entities

The Bureau of Indian Affairs, a DOI agency, is responsible for dams with high and significant hazard potentials on Indian reservations. The BIA maintains overall responsibility for the Safety of Dams Program and works with the Indian Tribes and Tribal Nations to operate and maintain those dams. Reclamation serves as the primary representative for all DOI bureaus and agencies, including the BIA, on the NDSRB, ICODS, and the Dams Sector GCC.

Relationships With Private Sector Organizations

Private national and international dam safety organizations have a significant influence on the Dams Sector:

- The Association of State Dam Safety Officials (ASDSO) is a national, not-for-profit organization of State and Federal dam safety regulators, dam owners and operators, and others interested in promoting dam safety. ASDSO is a member of the Dams SCC.
- The United States Society on Dams (USSD), formerly the U.S. Committee on Large Dams, was established in the early 1930s and is the nationwide professional organization focusing on dam and water resources development. USSD represents the

United States as one of the 83 member countries of the International Commission on Large Dams and has served as the private sector member of the NDSRB since its establishment in 1998. USSD is a member of the Dams SCC.

- The National Hydropower Association (NHA) is the national trade association committed exclusively to representing the interests of the hydroelectric power industry. NHA is a member of the Dams SCC.
- The National Water Resources Association (NWRA) is a federation of State water organizations in the 17 Western States representing municipal and agricultural water users. NWRA is a member of the Dams SCC.
- The Infrastructure Security Partnership was established after September 11, 2001, as a forum for U.S.-based public and private sector not-for-profit organizations to collaborate on issues involving the security of the Nation's built environment with regard to natural and manmade disasters.
- Many other national and international groups also have potential interests in Dams Sector issues: American Consulting Engineers Council; American Public Works Association; American Society of Civil Engineers; Associated General Contractors of America, Inc.; Association of State Floodplain Managers; Earthquake Engineering Research Institute; Electric Power Research Institute; International Association of Emergency Managers; National Emergency Management Association; National Governors Association; National Hazards Research and Applications Information Center; National Society of Professional Engineers; National Watershed Coalition; North American Electric Reliability Council; and the Portland Cement Association.

International Relationships

In the aftermath of the September 11, 2001, attacks, the U.S., Canadian, and Mexican governments focused a great deal of attention on their shared borders:

- In December 2001, the United States and Canada signed the Smart Border Declaration, which includes efforts to promote legitimate travel and commerce across the U.S.-Canadian border while protecting both countries from crime and terrorism.
- In March 2002, the United States and Mexico signed the Smart Border Declaration, which outlined specific actions to determine and address security risks while expediting the flow of legitimate goods and people across the U.S.-Mexican border.
- In November 2002, the United States and Mexico concluded the Critical Infrastructure Protection (CIP) Agreement to implement bi-national vulnerability assessments of trans-border infrastructure and communications and transportation networks to identify vulnerabilities and take protective measures. The CIP Agreement provides a cooperative framework under which bi-national guidelines are to be developed for critical infrastructure protection in six sectors under the general direction of the DHS and the Mexican Secretariat of Governance. One of these sectors, Dams/Water, has formed a working group, which is chaired by the IBWC (described earlier).
- On March 23, 2005, the United States, Canada, and Mexico entered into an unprecedented trilateral initiative—the Security and Prosperity Partnership of North America (SPP). SPP established a common security strategy to protect North America from external threats; prevent and respond to threats within North America; and further streamline the secure and efficient movement of legitimate, low-risk traffic across shared borders.
- In addition, the International Joint Commission was established by the 1909 Boundary Waters Treaty. More than 20 boards, made up of experts from the United States and Canada, help the commission carry out its responsibilities. In cases such as approving applications for dams or canals, the commission can set conditions limiting water levels and flows. After a structure is built, the commission may continue to play a role in how it is operated.

Relationships With Academia, Research Centers, and Think Tanks

The Dams Sector does not include academia, research centers, or think tanks as security partners. However, such organizations have been and will continue to be used on an as needed basis to improve dam security through research and development (R&D) efforts.

Section 2: Common Security Vulnerabilities

Introduction

Most dams are built according to well-documented engineering principles and regulated standards. They are designed to withstand a variety of potential problems (e.g., inherent structural flaws, failure of materials used to construct the dam, settling). A well-built large dam is relatively difficult to destroy. However, its vulnerability to disruption or destruction depends on the type of dam, the quality of construction and maintenance, and the type of control structures associated with the dam. While dam failures are fairly rare, failures have occurred.

The following pages list areas of potential vulnerabilities that could be found at some dams. These possible vulnerabilities are divided into those that are site-related and those that originate from interdependencies.

Site-related vulnerabilities are conditions or situations existing at a particular site that could be exploited by a terrorist or terrorist group to do economic, physical, or bodily harm or to disable or disrupt operations or critical infrastructures. Table 2-1 lists and describes several possible site vulnerabilities in the following categories: access and access control, operational security, SCADA and process control, and emergency planning and preparedness.

Whereas potential site-related vulnerabilities arise from the specifics of a particular site, interdependency vulnerabilities arise from the relationship between two or more sites or infrastructures by which the condition or functionality of each infrastructure is affected by the condition or functionality of the other(s). Interdependencies can be physical, geographic, logical, or information-based. Interdependencies potentially affecting natural gas and petroleum products, transportation, electric power, and telecommunications are described in table 2-2.

Many dam owners have instituted security programs based on risk-based management decisions to improve security performance, including provisions to increase security measures or postures during heightened threat conditions.

No universal list of vulnerabilities applies to all assets within the Dams Sector. The vulnerabilities listed in tables 2-1 and 2-2 should be interpreted as possible vulnerabilities.

Table 2-1: Site-Related Potential Vulnerabilities	
Access and Access Control	
1	Dams may experience large numbers of visitors because of associated water-based recreation and, in some cases, the dam is a tourist attraction.
2	Public roads or rail lines may pass through, pass over, or be adjacent to some sites, and larger dams often have a road along the top.
3	Dams are typically accessible by water, allowing possible water-borne or waterside attack.
4	Access to critical assets (e.g., control rooms, powerhouses, and transmission equipment) is generally controlled through gates, doors, and fences that may not be adequately protected.
5	Critical assets (e.g., control areas) may be close to the perimeter fence.
6	Critical assets (e.g., transformers) may be partially exposed or out in the open.
7	Dams may be unguarded or have unarmed security guards.
8	Access controls based on cards or badges might not positively identify the user.
9	Employee and visitor parking may be located adjacent to critical buildings.
10	Lighting and monitoring of entrance points may be limited.
11	Intrusion detection system (IDS) and closed-circuit television (CCTV) configurations to detect and assess intrusion into restricted areas (including water areas) may be in need of updating or realignment.
12	Critical assets might not be adequately protected.
13	Dams may be located in remote, rural, or semi-rural locations.
14	Procedures to inspect vehicles for explosives and/or dangerous materials before allowing such vehicles to enter the dam area may need to be updated.
15	Dams may use contract guard services that vary in the quality of support.
16	Signs posted to deter vehicles, boats, or pedestrians from entering unauthorized portions of the premises might be missing or damaged.
17	CCTV assessment might not fully cover some critical assets.
18	Lighting, in support of CCTV assessment, may be limited.
Operational Security	
19	Background checks on employees and contractor personnel may be limited.
20	Coordination among local, State, and Federal agencies on roles/responsibilities for security and/or response might be limited.
21	Information on locations, assets, maps, and other operational data might be available in open literature and on the Internet.
22	Procedures might not be in place for inspection of deliveries.
23	Procedures or mechanisms might not be in place to cut power to assets (e.g., spillway gates, outlet works, intake structures).

(*Table 2-1, continued*)

SCADA and Process Control	
24	Policies, procedures, and culture governing control systems security might need to be updated.
25	Designed control system networks might benefit from updated defense-in-depth mechanisms.
26	Remote access to the control system might be better controlled.
27	Auditable system administration mechanisms (e.g., system upgrades, user metrics) might not automatically be part of the control system.
28	Wireless communications security might need to be upgraded.
29	Non-dedicated communications channels for command and control might be used.
30	Quick and easy tools to detect and report on anomalous or inappropriate activity might be outdated.
31	Inappropriate applications may be installed on the host computers for control systems.
32	Software used in control systems might not have been adequately scrutinized for vulnerabilities.
33	Control systems command and control data might not be authenticated.
34	Backup control centers or backup instructional codes within process control devices might not be regularly maintained.
Emergency Planning and Preparedness	
35	Response times for emergency response and law enforcement agencies might be relatively long.
36	Coordination of emergency action plans (EAPs), rapid recovery plans (RRPs), or site-specific security plans (SSSPs) with local, State, Federal, tribal, and international governments might be limited.
37	Spare parts that are large and/or expensive and/or unique might be in short supply.
38	Fires or explosions could present difficult challenges to first responders.

Table 2-2: Potential Interdependency Vulnerabilities	
General Vulnerability	
1	Failure of the flood control mission at one dam may lead to failure at downstream facilities.
Natural Gas/Petroleum Products	
2	Assets may have backup diesel generators that rely on delivered fuel.
Transportation	
3	Maintenance and repair of dams (e.g., hydroelectric facilities) require the movement of personnel, equipment, and often heavy-duty vehicles (e.g., cranes) over distances that can be significant.
4	The dam may rely on different transportation systems, including road, rail, and waterway. Loss or disruption of these systems may reduce or shut down operations or may inhibit effective implementation of emergency procedures (e.g., evacuation, emergency response).
5	Public roads may run across some dams.
Electric Power	
6	Electric power is needed for SCADA, water control system operations, and security systems.
7	Larger dams may have water-powered generators devoted to the internal electricity supply (known as “station service units”) with diesel backup. Switches and transformers associated with station service units might not be secured.
8	Multiple organizations may be involved in providing electrical service to the dam and may have different degrees of security.
Telecommunications	
9	Mobile telecommunications may be needed for communications between security units (e.g., between a gate guard and the control room).

Section 3: Potential Indicators of Threat Activity

Introduction

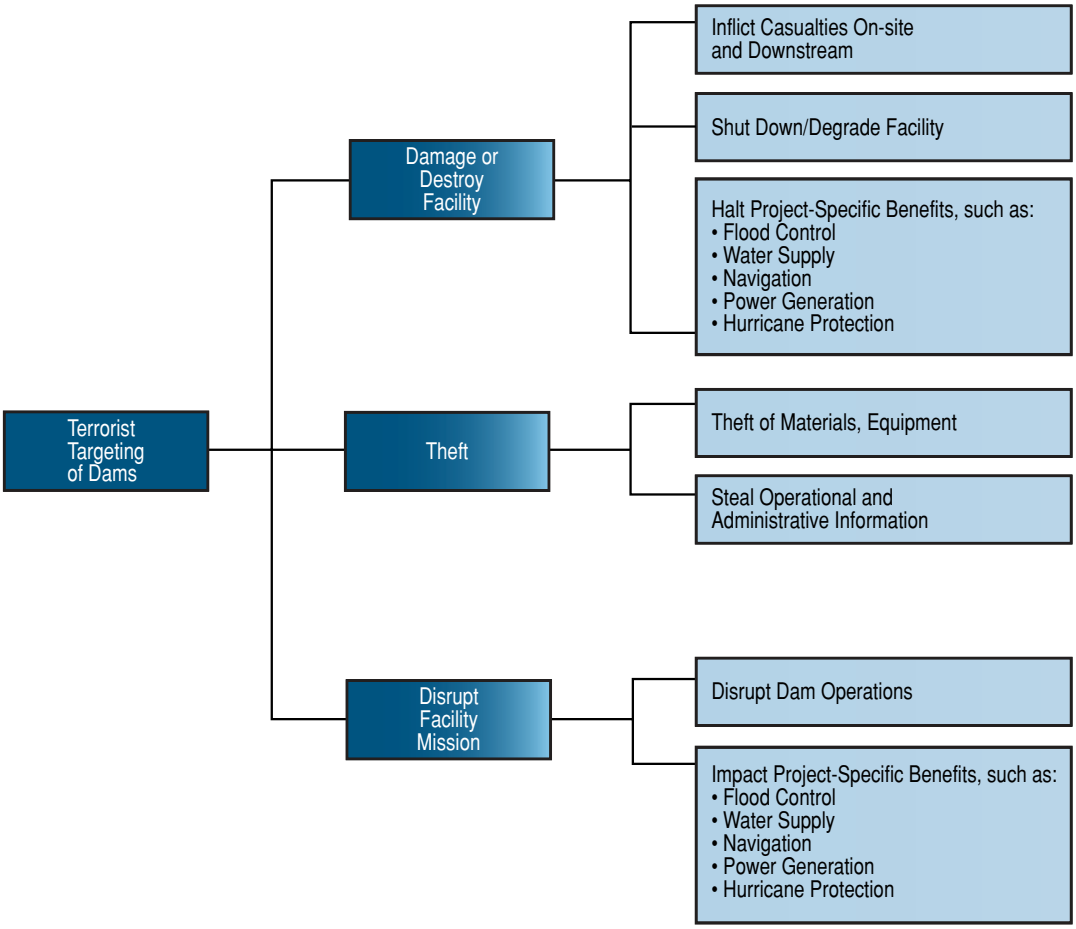
Threats can be posed by an individual or a group that possesses the capability and intent to do harm. Domestic and international terrorists, adversary nations, disaffected individuals or groups, disgruntled employees, and organized adversarial groups are all potential sources of threats against critical infrastructure targets. While there is no history or credible intelligence to suggest that domestic dams are viable terrorist targets, threats can originate from individuals or groups with knowledge of the systems and equipment used in the Dams Sector. Insider information could be held by disgruntled or compromised employees within the United States, while detailed information on equipment and operating procedures can also be gathered from open sources or from active or former employees.

In targeting critical infrastructure, potential adversaries can employ a wide range of weapons, tools, and tactics, including the possible use of explosives. Some antagonists could potentially use less traditional methods, such as cyber attacks. Attacks of this nature would involve the use of digital control and information systems to deny, exploit, corrupt, or destroy a target's resources. As critical infrastructure and business systems rely increasingly on interconnected computer systems, the need for secure telecommunications intensifies.

A common framework for assessing threats involves identifying the threat purveyor's objectives and goals, potential targets, the means by which a threat might be carried out, and the knowledge and tactics required to carry out the threat. Understanding those factors, and why a dam would be targeted, leads to identifying what types of activity are suspicious and could be indicators of a possible threat.

One of the goals of the *Dams Sector Security Awareness Handbook* is to develop a common understanding of what kind of activity at or around dams is considered suspicious and should be reported to the response community. Dams can be attractive terrorist targets because of the potential for dramatic effects, such as the destruction of a major dam, the potential for downstream damage and casualties from flooding, and the loss of project-specific benefits, as depicted in figure 3-1.

Figure 3-1: Terrorist Targeting Objectives



What Is an Indicator of a Possible Threat?

An indicator could be any suspicious activity that warrants a reaction. A reaction could be an investigation, root-cause analysis, communication, or an emergency response.

Owners and operators should watch for and be aware of suspicious activities that can include something out of place, unusual or odd behavior of employees or visitors, unattended objects, inventory control issues, distribution issues, and unexplained equipment or process failures. Constant attention to these indicators can help to alert officials of the possibility of an incident.

The section below on surveillance and suspicious activity indicators is followed by sections describing indicators of possible weapons; explosives; or chemical, biological, or radiological threats. The series of tables in those sections outline additional indicators of possible surveillance activity or focus. While the tables are fairly voluminous in nature, the key for owners and their employees is to be familiar with activities normally associated with a given asset and recognize when unusual events occur so that they can be reported appropriately as outlined in the next section.

Surveillance Objectives and Indicators, and Indicators of Suspicious Activity

Surveillance is used by terrorists to identify and plan their attack on a facility. In the past, terrorist surveillance has been conducted over an extended period of time in order to identify vulnerabilities and plan the best means to attack the target. Because of their generally remote location, dams present a more difficult surveillance challenge than facilities in a more urban setting.

This gives dam owners and operators, as well as law enforcement officials in the vicinity of dams, an opportunity to detect such surveillance before dams could be targeted.

The objectives of surveillance are listed in table 3-1. Understanding the signature behaviors associated with terrorist operational planning will help infrastructure security personnel better capture real and perceived terrorist surveillance efforts in suspicious incident reporting, which may ultimately lead to the disruption of potential terrorist attack planning.

Table 3-1: Surveillance Objectives

Surveillance and Counter-Surveillance
Identify:
- Places where further surveillance can take place
- Places where counter surveillance can be detected

Facility Security
Identify:
- Presence or absence of security cameras
- Number, location, type, and coverage of security cameras
- Security screening procedures for employees, visitors, and vehicles
- Changing-of-the-guard procedures
- Facility identification cards or special license plates
- Proximity to first-responder locations
- Security event response times
- Number, gender, ethnicity, location, dress, weapons, and equipment of private and police security coverage

Facility Access
Identify:
- Configuration and staffing of control points
- Visitor access procedures
- Availability of tours
- Location of roadways, entrances, parking lots, gates, and access points

Facility Construction
Identify:
- Construction materials used
- Building shape, height, and setbacks
- Location of vulnerable structural components
- Opportunities for cascading damage effects
- Location of executive offices and employee meeting places
- Location of power and heating, ventilating, and air-conditioning (HVAC) systems
- Adequacy of emergency exits, escape routes, and fire suppression systems

Target Dynamics
Identify:
- Opening and closing times
- Lunch and break times
- Shift changes
- Patterns of concentration of people and vehicles, traffic congestion
- Nearby people and vehicle movement throughout the day
- Police radio frequencies and recording of emergency response times

Secondary Targets
Identify:
- Nearby alternative targets
- Nearby collateral targets

Terrorist surveillance may be fixed or mobile. Fixed surveillance is performed from a static, often concealed position, possibly an adjacent building, business, fishing pier, bridge, or other adjacent location. Terrorists may establish themselves in a public location over an extended period of time or choose disguises or occupations, such as tourists, fishermen, campers, repair or delivery persons, photographers, or even demonstrators, to provide a plausible reason for being in the area. Dam owners and operators are generally familiar with the persons and activities that occur in the vicinity of their dams and should be alert for changes in routine or persons suddenly showing an interest in their dam.

Mobile surveillance usually entails observing and following persons or individual human targets, although it can be conducted against non-mobile facilities (i.e., driving by a site to observe the facility or site operations).

More sophisticated surveillance is likely to be accomplished over a long period of time. This type of surveillance tends to evade detection and improve the quality of gathered information. Some terrorists perform surveillance of a target or target area over a period of months or even years. Public parks and other public gathering areas provide convenient venues for surveillance because it is not unusual for individuals or small groups in these areas to loiter or engage in leisure activities that could serve to cover surveillance activities. 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.

Terrorists are also known to use advanced technology, such as modern optoelectronics, communications equipment, video cameras, and other electronic equipment. Such technologies include commercial and military night-vision devices and global positioning systems. It should be assumed that many terrorists have access to expensive technological equipment.

Electronic surveillance, in this instance, refers to information gathering, legal and illegal, by terrorists using off-site computers. This type of data gathering might include obtaining asset maps, key locations, security procedures, or passwords to company computer systems. In addition to obtaining information that is useful for a planned physical attack, terrorists may launch an electronic attack that could affect (e.g., damage or modify) data, software, or equipment/process controls (e.g., cause a dangerous release by opening or closing a valve using off-site access to the SCADA system). Terrorists may also use technical means to intercept radio or telephone (including cell phone) traffic.

An electronic attack could be an end in itself or could be launched simultaneously with a physical attack. Thus, it is worthwhile to be aware of what information is being collected from company and relevant government Web sites by off-site computer users and, if feasible, who is collecting this information. In addition, it is important to know whether attempts are being made to gain access to protected company computer systems and whether any attempts have been successful.

The surveillance indicators listed in table 3-2 are examples of unusual activities that should be noted and considered as part of a process that takes into account the quality and reliability of the source, the apparent validity of the information, and how the information meshes with other information at hand. Table 3-2 also lists indicators of suspicious activity that could be related to an act of terrorism.

Table 3-2: Surveillance Indicators and Indicators of Suspicious Activity Observed at or Near a Dam	
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 a 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 use, 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 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.
Indicators About Activities (Observed or Reported)	
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	Repeated attempts from the same location or country to access protected computer information systems.
18	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.
19	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).
20	Unfamiliar cleaning crews or other contract workers with passable credentials, crews or contract workers attempting to access unauthorized areas.
21	A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
22	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).

(*Table 3-2, continued*)

23	Sudden increase in power outages. Outages could be implemented from an off-site location to test the backup systems or recovery times of primary systems.
24	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.
25	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.
26	Traces of explosive or radioactive residue on vehicles during security checks by personnel using detection swipes or devices.
27	Increase in violation of security guard standard operating procedures for staffing key posts.
28	Increase in threats from unidentified sources by telephone, by postal mail, or through the email system.
29	Increase in reports of threats from outside known, reliable sources.
30	Sudden losses or theft of guard force communications equipment.
31	Displaced or misaligned manhole covers or other service access doors on or surrounding the asset site.
32	Unusual maintenance activities (e.g., road repairs) near the asset.
33	Observations of unauthorized personnel collecting or searching through trash.
34	Unusual packages or containers, especially near HVAC equipment or air-intake systems.
35	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
36	Packaging and/or packaging components that are inconsistent with the usual shipping mode.
37	Delivery of equipment or materials that is unexpected, unusual, out of the norm, without explanation, or with suspicious or missing paperwork.
38	Excessive requests or interest in access for deliveries or pickups.
39	Vendors or suppliers make unusual requests concerning the shipping or labeling of deliveries.

Weapons; Explosives; and Chemical, Biological, or Radiological Indicators

Suspicious activities involving weapons; explosives; or chemical, biological, or radiological threats may also warrant reactions at an appropriate level.

Weapons

Indicators of the possible use of weapons against a dam include the purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out an intended action. Items of interest include not only guns, automatic weapons, and rifles, but also ammunition, equipment (e.g., night-vision goggles and body armor), and relevant training exercises and classes. Table 3-3 briefly expands on this description of weapons indicators.

Table 3-3: Weapons Indicators at or Near a Dam

Indicators About Activities (Observed or Reported)	
1	Reports of automatic weapons being fired or the firing of unusual weapons.
2	People wearing clothing that is not consistent with the local weather.
3	Training scenarios carried out by paramilitary groups or other organizations advocating violence.
4	Theft, transactions, or seizures of large numbers of automatic or semi-automatic weapons, ammunition capable of being used in military weapons, modified weapons or equipment used to modify weapons (e.g., silencers), large-caliber sniper weapons, night-vision equipment, and body armor, especially in combination with other indicators.

Explosives

Indicators of explosive or incendiary materials and devices that could be used by terrorists include production, purchase, theft, testing, or storage of any of these types of materials. Table 3-4 describes indicators of those activities in addition to indicators of vehicle-borne improvised explosive devices (VBIEDs). VBIEDs are dangerous because they are inherently mobile, inconspicuous by design, and conceal large amounts of explosives, which imply that they do not always have to penetrate perimeter security defenses to be effective. The VBIED indicators listed in table 3-4 are taken from lessons learned in Iraq.

Table 3-4: Explosive and Incendiary Indicators at or Near a Dam	
Indicators About People (Observed or Reported)	
1	Persons stopped or observed with unexplained amounts of explosives.
2	Unidentified persons making inappropriate inquiries regarding explosives or explosives construction.
3	Treated or untreated chemical burns or missing hands and/or fingers.
Indicators About Activities (Observed or Reported)	
4	Thefts, transactions, or seizures of large amounts of smokeless powder, blasting caps, high-velocity explosives, or combinations of ingredients for explosives (e.g., fuel oil, nitrates).
5	Thefts, transactions, or seizures of large amounts of high-nitrate fertilizer.
6	Thefts, transactions, or seizures of containers (e.g., propane bottles) or vehicles (e.g., trucks, cargo vans) in combination with other indicators.
7	Reports of explosions, particularly in rural or wooded areas.
8	Traces of explosive residue on visitor or business vehicles during security checks by personnel using explosive detection techniques.
9	Thefts, transactions, or seizures of improvised explosive devices.
10	Thefts, transactions, or seizures of explosives or restricted or sensitive chemicals.
11	Theft of sedan, passenger/cargo van, delivery truck, moving van, water truck, or semi-trailer with the ability to carry small to large amounts of explosives.
12	Modification of sedan, passenger/cargo van, delivery truck, moving van, water truck, or semi-trailer with the ability to carry small to large amounts of explosives.
13	Rental of self-storage units or out-buildings and delivery of chemicals or suspicious materials to such units.
14	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in storage out-buildings; in nearby homes, apartments, or hotel rooms; or in self-storage units.
15	Suspicious packages, especially unexpected deliveries with no return address or an unknown return address and/or with excessive postage.
16	Unattended packages, briefcases, or other containers.
17	Unexpected or unfamiliar delivery trucks or deliveries.
18	Vehicles containing unusual or suspicious parcels or materials.
19	Unattended vehicles on or off site in suspicious locations or at unusual times.
Indicators about VBIEDs	
20	Noticeable sagging of the vehicle on its springs caused by the heavy weight of explosives. Ordinarily, explosives are placed toward the rear of the vehicle, causing it to ride lower in the rear. However, sagging springs are not normally characteristic of commercial trucks carrying VBIEDs because these vehicles are designed to carry the weight.
21	Darkened or covered windows to conceal either the vehicle's contents or the driver's actions.
22	Unusual items inside the vehicle: gas cylinders, wires, leaflets, large bags or boxes, and batteries, except for the normal car battery.

(*Table 3-4, continued*)

23	Indications of a triggering device (i.e., a switch, radio transmitter, timer, wires, or ropes passing from the front seat to the rear of the vehicle) visible near the driver, under the seat, or within arm's reach.
24	Presence of the vehicle in an area where it should not be, perhaps illegally parked.
25	Holes made in the vehicle body to hide explosives and then crudely covered.
26	Evidence that an interior door panel has been removed to hide explosives.
27	Presence of powder or prills (small rounded granular material) left when explosive material was loaded into the vehicle.
28	Recent painting of the vehicle to cover body alterations.
29	Additional fuel tanks (used to hide explosives or provide additional gasoline to fuel an explosive event).
30	Unusual smells (e.g., burning time fuse, gasoline, or fertilizer).
31	Additional antennas on the vehicle for radio-controlled devices.
32	Any disturbance to the undercoating or dirt on the bottom of a vehicle.

Chemical, Biological, and Radioactive Materials

Chemical agents, biological species, and hazardous radioactive materials could also be a threat to dams. Indicators of the possible presence of these materials are related to production, purchase, theft, testing, or storage and are described in table 3-5.

Table 3-5: Chemical, Biological, and Radiological Indicators at or Near a Dam

Equipment Configuration Indicators	
1	An area under strict security control, such as an area close to a dam, where equipment is being installed or material is being stored, that is inconsistent or out of character.
2	Suspicious packages, especially unexpected deliveries with no return address or an unknown return address and/or with excessive postage.
3	Unattended packages, briefcases, or other containers.
4	Unexpected or unfamiliar delivery trucks or deliveries.
5	Vehicles containing unusual or suspicious parcels or materials.
6	Thefts, transactions, or seizures of sophisticated personal protective equipment (e.g., A-level Tyvek®, self-contained breathing apparatus, etc.).
7	Thefts, transactions, or seizures of sophisticated filtering, air-scrubbing, or containment equipment.
Chemical Agent Indicators	
8	Inappropriate inquiries regarding chemical usage, transactions, storage, or transportation.
9	Thefts, transactions, or seizures of explosives or restricted or sensitive chemicals.
10	Rental of self-storage units or out-buildings and delivery of chemicals to such units.
11	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in storage out-buildings; in nearby homes, apartments, or hotel rooms; or in self-storage units.
12	Treated or untreated chemical burns or missing hands and/or fingers.
13	Unusual packages or containers, especially near HVAC equipment or air-intake systems.
14	Unusual powders, droplets, or mist clouds near HVAC equipment or air intake systems.
Biological Agent Indicators	
15	Thefts, transactions, or seizures of large quantities of baby formula (a medium used to grow biological agents).
16	Break-in at or tampering of nearby water treatment facility or food processing/warehouse facility.
17	Solicitation for sale or theft of live agents/toxins/diseases from medical supply companies or testing/experiment facilities.
18	Thefts, transactions, or seizures of unexplained lethal amounts of agents/toxins/diseases/explosives.
19	Multiple cases of unexplained human or animal illnesses, especially those illnesses not native to the area.
20	Large number of unexplained human or animal deaths.
21	Thefts or transactions (especially by non-agricultural users) of agricultural sprayers or crop-dusting aircraft, foggers, river craft, or other dispensing systems.
22	Inappropriate inquiries regarding biological agent usage, transactions, storage, or transportation.
23	Inappropriate inquiries regarding heating and ventilation systems for facilities by persons not associated with service agencies.

(*Table 3-5, continued*)

24	Unusual packages or containers, especially near HVAC equipment or air-intake systems.
25	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
Radioactive Material Indicators	
26	Break-in at or tampering of facilities storing radioactive materials or radioactive waste.
27	Solicitation for sale or theft of radioactive materials from medical or research supply companies or from testing/experiment facilities.
28	Thefts, transactions, or seizures of unexplained radioactive materials.
29	Any one or more cases of unexplained human or animal radiation burns or radiation sickness.
30	Large number of unexplained human or animal deaths.
31	Inappropriate inquiries regarding usage, transactions, storage, or transportation of radiological materials.

Section 4: Reporting of Incidents

Communications Process

The process for how the Dams Sector security partners and the response community share information is an integral part of any effort to develop successful and ongoing relationships. Dam owners and operators are encouraged to establish and maintain effective relationships with the law enforcement agency or agencies that provide service in their area. They should also have ongoing relationships with other dam owners, particularly those with upstream or downstream impacts.

Suspicious incidents, such as suspected surveillance activities, should promptly be reported to the local law enforcement agencies and the local Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF). (Space was provided in the front of this handbook to record those numbers.) Dam incidents of an immediate nature, such as an attack on a facility, should be immediately reported via a 911 call. Dam owners should ensure that they have internal protocols in place to ensure such reporting and coordination.

It is necessary to understand how suspicious activities are reported and to understand the existing linkages among regional industries, local law enforcement, fire service, hazardous materials (HAZMAT) responders, regional FBI weapons of mass destruction (WMD) coordinators, U.S. Coast Guard (USCG), the local JTTF, and other authorities having jurisdiction.

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.

Depending on the situation, additional contacts may include:

- Local FBI office;
- State Dam Safety Office;
- County sheriff or local law enforcement;
- State emergency management (especially if State regulated);
- FERC regional office, if FERC regulated;
- Owner and licensee of the dam;
- USCG;
- Electricity Sector and/or Water Industry Information Sharing and Analysis Centers (www.esisac.com, www.waterisac.org);
- U.S. Environmental Protection Agency (EPA) regional office;
- Downstream dam operator; and
- Upstream dam operator.

Owners and operators of dams should have an EAP, an RRP, and an SSSP that outline an emergency notification process for different levels of threat that is consistent with business and regional emergency procedures.

Event Reporting Criteria

The communications process starts with identifying a suspicious security-related activity or incident. Criteria for determining what activities or incidents to report include:

- Terror/bomb threats;
- Unauthorized access;
- Suspicious inquiries;
- Theft or acquisition of materials associated with explosive devices;
- Presence of detailed diagrams and notes about buildings or facilities;
- Suspicious mail;
- Incident or activity resulting in extended service outage;
- Discovery or appearance of suspicious bomb-making materials;
- Presence of weapons such as rifles, rocket launchers, explosives, poisons, or precursor materials;
- Physical surveillance;
- Cyber surveillance;
- Security breaches; and
- Planting/pre-positioning malicious code.

How to Provide an Accurate Report

There are two key elements in preparing a good report: accuracy and timeliness.

- *Accuracy* means reporting the facts. The facts should not be embellished to make the situation seem more important. It is appropriate to include the reason that the activity seemed suspicious, even if the rationale is that the activity was something out of the ordinary. An explanation of why the activity was not "normal" should be provided with specificity. Any conclusion needs to be supported by the facts.
- *Timeliness* is critical. As time passes, the ability of the suspicious person or persons to escape and avoid apprehension increases. Appearances can be altered and evidence can be destroyed or hidden for later retrieval. It is very important to report anything suspicious immediately after it is observed and, if possible, while the suspicious activity is occurring and the perpetrator is present.

What to Report

It is important to provide as much information as possible to the responding officers, for example, by trying to create a "word picture" to help people visualize the person, place, or thing being described. A description of this nature will assist law enforcement personnel in their response and followup investigation. The ability to distinguish among details that will remain constant and those that will change on the basis of time, weather, or intentional acts by the suspicious person or persons should be noted.

When reporting suspicious behavior or circumstances, it is important to include as much of the following information as possible:

- **Who?** Identify yourself. Describe the person or persons involved in the suspicious activity.
- **What?** Describe the suspicious activity. Indicate if there is an immediate threat to persons nearby or to responding officers (e.g., the presence of weapons or HAZMAT).
- **When?** Indicate whether the activity is in progress or how much time has elapsed since the activity ended. Provide the exact time(s) that the activities occurred.
- **Where?** Give your location, the location of the suspicious activity, and the location of the suspect(s).
- **Why?** Explain why the activity seems suspicious to you. If known, tell what could be the target of the activity.
- **How?** Describe how the suspicious act(s) were carried out, including methods or techniques.

Effective information collection enables faster and more thorough investigative followup. It is not always possible to gather detailed incident information; however, collecting the following types of information will facilitate the investigative and analytic process:

- Date and time of incident
- Number of individuals involved
- Name and address of the facility
- Description of the incident, with a description of the business function of the facility involved

For suspicious persons:

- Name(s) and aliases, including variations in spelling
- Physical description, including:
  - Gender
  - Race
  - Size/build

  - Height
  - Scars, marks, or tattoos
  - Skin color
  - Disabilities
  - Hair color
  - Presence or absence of facial hair
  - Eye color
  - Hair style
  - Clothing
- Social Security number and any passport/visa information
- Reason for being in the area or conducting the suspicious activity
- Place of employment
- Copy of picture ID(s)
- History of incidents with this individual, especially at this facility

For vehicles:

- Physical description, including:
  - Make (e.g., Ford, Toyota)
  - Model (e.g., Focus, Celica)
  - Type of vehicle (e.g., passenger car, sport-utility vehicle, van)
  - Year
  - License plate number and State
  - Color
  - Markings (designs, company names)
  - Accessories (running lights, unusual wheels/tires, trailer)
  - Damage
  - Distinguishing marks, stickers, and embellishments
- Number and description of occupants
- Materials or items carried
- History involving the same vehicle, especially at this facility

For aircraft:

- Physical description, including:
  - Type of plane (passenger, commercial)
  - Prop, jet engine, helicopter, glider

  - Tail number
  - Color scheme
- Smoke, mist, or clouds streaming from the plane
- Number and description of occupants
- Materials or items carried
- History involving the same plane, especially at this facility

For boats:

- Physical description, including:
  - Boat registration ID
  - Type of boat (pontoon, commercial fishing, jet ski)
  - Size
  - Inboard or outboard motor
  - Color scheme
  - Markings (designs, names)
  - Other identifying information
- Number and description of occupants
- Materials or items carried
- History involving the same boat, especially at this facility

For suspect's surveillance equipment:

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

Describe any other suspicious individuals in the vicinity. Provide contact information for the reporting individual, witnesses, and the organization or facility.

Elements of local law enforcement or other Federal, State, or local agencies that have been notified are responsible for:

- Follow-up actions
- Results of follow-up actions
- Points of contact for further information

Once the response community has been contacted about the suspicious activity, you will be expected to answer some basic questions. It would benefit the response community if you were prepared to provide answers as soon as possible for the following questions:

- What equipment was stolen, lost, found missing?
- How did you discover that the items were missing?

- Did anyone notice any suspicious people or occurrences nearby?
- Why is the activity being reported considered suspicious?
- How could the activity inflict harm on personnel or infrastructure?
- Are there recommended precautions for dealing with stolen material?
- Can you provide contact information for experts in the Dams Sector?
- Has this suspicious activity been reported to any other agency?

Summary

This handbook is intended to provide dam owners and operators with information to increase their security awareness in general. Owners are encouraged to maintain effective relationships with their local law enforcement community and to have effective and up-to-date emergency action plans that include exercises and training with first-responders, other dam owners, and other appropriate parties. They are also encouraged to have internal notification protocols and education programs to ensure that suspicious activities or actual incidents are recognized and promptly reported.

Dams Sector security partners must take the initiative to foster these working relationships before an event occurs.

Appendix A: Key Definitions

Title 18 of the United States Code (U.S.C.), Chapter 118b, Section 2331, defines international and domestic terrorism. These definitions are provided below.

International Terrorism

International terrorism consists of "activities that involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping; and occur primarily outside the Territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum."

Domestic Terrorism

Domestic terrorism consists of "activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping; and occur primarily within the Territorial jurisdiction of the United States."

Appendix B: Important Federal Initiatives Supporting Security Matters for the Dams Sector

National Infrastructure Protection Plan

The ability to protect the CIKR of the United States is vital to our national security, public health and safety, economic vitality, and way of life. U.S. policy focuses on the importance of enhancing CIKR protection to ensure that essential governmental missions, public services, and economic functions are maintained in the event of a terrorist attack, natural disaster, or other type of incident, and that those elements of CIKR are not exploited for use as weapons of mass destruction against our people or institutions.

The Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 (HSPD-7) provide the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CIKR. The act assigns the DHS the responsibility for developing a comprehensive national plan for securing CIKR and for "coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities" in the development of CIKR Sector-Specific Plans. This national plan, released in June 2006, is called the National Infrastructure Protection Plan (NIPP); Sector-Specific Plans (SSPs) were released in 2007. Table B-1 lists the 17 CIKR sectors and the agencies assigned to each.

Together, the NIPP and SSPs provide the mechanisms for establishing security goals and priorities within each sector; identifying critical facility features and functions; understanding threats; assessing vulnerabilities and consequences; prioritizing protection initiatives and investments on the basis of costs and benefits to target the greatest mitigation of risk; and enhancing information-sharing mechanisms and protective measures within and across CIKR sectors. The NIPP and SSPs are expected to evolve and adapt over time.

The development of SSPs is an enormous and complex task under the responsibility of the designated Sector-Specific Agencies (SSAs). To be effective, organizational structures and partnerships were formed between the SSAs and their sectors, which are committed to sharing and protecting the information needed to achieve the NIPP goals and development of SSPs. These include two councils:

- Sector Coordinating Councils (SCCs) are comprised of private sector representatives.
- Government Coordinating Councils (GCCs) are comprised of representatives of Federal departments and agencies and of State, local, and tribal governments.

These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing consensus approaches to CIKR protection.

Cross-sector entities were also established to promote coordination, communications, and sharing of best practices across CIKR sectors, jurisdictions, or specifically defined geographic areas.

Table B-1: Critical Infrastructure, Key Resources, and Sector Agencies

Critical Infrastructure	Agriculture and Food	USDA	Sector-Specific Agencies
	Public Health and Healthcare	HHS	
	Drinking Water and Water Treatment	EPA	
	Defense Industrial Base	DOD	
	Energy	DOE	
	Banking and Finance	TREAS	
	National Monuments and Icons	DOI	
	Information Technology	DHS	
	Telecommunications	DHS	
	Transportation Systems	DHS	
	Chemical	DHS	
	Emergency Services	DHS	
	Postal and Shipping	DHS	
Key Resources	Dams	DHS	
	Commercial Facilities	DHS	
	Government Facilities	DHS	
	Commercial Nuclear Reactors, Materials, and Waste	DHS	

Note: Acronyms used in table B-1 are defined in appendix G.

Cross-sector issues and interdependencies are addressed among the SCCs through:

- The Partnership for Critical Infrastructure Security (PCIS). PCIS membership is comprised of one or more members and their alternates from each of the SCCs.

Cross-sector issues and interdependencies between the GCCs are addressed through:

- The Government Cross-Sector Council, which is comprised of: (1) the NIPP Federal Senior Leadership Council, and (2) the State, Local, and Tribal Government Cross-Sector Council.

Continued cooperation and collaboration between and among these security partners is critical to the successful implementation of these plans.

The 2007 Dams Sector-Specific Plan lists the following sector security goals:

1. Build Dams Sector partnerships and improve communications among all sector security partners;
2. Identify Dams Sector composition, consequences, and critical assets;
3. Improve the Dams Sector's understanding of viable threats;
4. Identify Dams Sector vulnerabilities;
5. Identify risks to Dams Sector critical assets;
6. Develop guidance on how the Dams Sector will manage risks;
7. Enhance the security of the Dams Sector through research and development efforts; and

8. Identify and address interdependencies.

Protected Critical Infrastructure Information

Effective information-sharing and information-protection processes based on trusted relationships help to ensure implementation of CIKR programs. Information sharing enables both government and private sector security partners to assess risks, conduct risk management activities, allocate resources, and make continuous improvements to the Nation's CIKR protective posture.

The Critical Infrastructure Information Act of 2002 was passed to encourage the voluntary submission of critical infrastructure information by the private sector by creating a category of information called, Protected Critical Infrastructure Information (PCII). PCII is information that:

- Has been **voluntarily** submitted to a PCII Program Office (within the DHS);
- Is validated by a PCII Program Office;
- Is not otherwise available to the Federal Government;
- Is not customarily in the public domain;
- Is protected from disclosure under the Freedom of Information Act; and
- Is only made available to authorized users certified for PCII.

Safeguarding and handling of PCII is vitally important because:

- Industry has voluntarily provided the information with the understanding that it will be protected;
- The information may contain proprietary information that is vital to a company's continued success;
- If information is not adequately protected, companies will not share it; and
- If information is not provided, the Intelligence Community, law enforcement agencies, and protective programs will lack a key analytical tool.

The rules for handling, safeguarding, transporting, communicating, and using PCII are strict and may include fines and imprisonment for mishandling. Authorized users, including the States and State entities, are subject to disclosure agreements and periodic certification. The sanctions against Federal employees and contractors are severe; however, those same sanctions do not apply to non-Federal recipients.

PCII protections exist only for information provided by a dam owner or operator voluntarily. Owners should be aware that once information is provided to the DHS, it may be shared with other agencies.

Appendix C: Selected Executive Orders (EOs), Presidential Decision Directives (PDDs), and Homeland Security Presidential Directives (HSPDs)

EO 12148
Federal Register, Volume 44, page 43239 (44 FR 43239), 1979, as amended by EO 13286, 68 FR 10619 (2003), designates the Department of Homeland Security as the primary agency for the coordination of Federal disaster relief, emergency assistance, and emergency preparedness. The order also delegates the President's relief and assistance functions under the Stafford Act to the Secretary of Homeland Security, with the exception of the declaration of a major disaster or emergency.
EO 12656
53 FR 47491 (1988), Assignment of Emergency Preparedness Responsibilities, as amended by EO 13286, 68 FR 10619 (2003), assigns lead and support responsibilities to each of the Federal agencies for national security emergency preparedness. The amendment designates the Department of Homeland Security as the principal agency for coordinating programs and plans among all Federal departments and agencies.
EO 13354
69 FR 53589 (2004), National Counterterrorism Center, establishes policy to enhance the interchange of terrorism information among agencies and creates the National Counterterrorism Center to serve as the primary Federal organization in the U.S. Government for analyzing and integrating all intelligence information posed by the United States pertaining to terrorism and counterterrorism.
EO 13356
69 FR 53599 (2004), Strengthening the Sharing of Terrorism Information to Protect Americans, requires the Director of Central Intelligence, in consultation with the Attorney General and the other intelligence agency heads, to develop common standards for the sharing of terrorism information by agencies within the Intelligence Community with: (1) other agencies within the Intelligence Community; (2) other agencies having counterterrorism functions; and (3) through or in coordination with the Department of Homeland Security, the appropriate authorities of State and local governments.
PDD-39
U.S. Policy on Counterterrorism, June 21, 1995, establishes policy to reduce the Nation's vulnerability to terrorism; deter and respond to terrorism; and strengthen capabilities to detect, prevent, defeat, and manage the consequences of terrorist use of weapons of mass destruction; and assigns agency responsibilities. (PDD 39 superseded by HSPDs)
PDD-62
Combating Terrorism, May 22, 1998, reinforces the missions of Federal departments and agencies charged with roles in defeating terrorism. (PDD 62 superseded by HSPDs)
PDD-63
Protecting America's Critical Infrastructures, May 22, 1998, makes it the policy of the U.S. Government to lead a public/private partnership aimed at eliminating all major vulnerabilities to the Nation's critical physical and cyber infrastructures. (PDD 63 superseded by HSPDs)
HSPD-1
Organization and Operation of the Homeland Security Council, October 29, 2001, establishes policies for the creation of the Homeland Security Council, which shall ensure the coordination of all homeland security-related activities among executive departments and agencies, and promote the effective development and implementation of all homeland security policies.

(*Table continued from previous page.*)

HSPD-2
Combating Terrorism Through Immigration Policies, October 29, 2001, mandates that, by November 1, 2001, the Attorney General is to create the Foreign Terrorist Tracking Task Force, with assistance from the Secretary of State, the Director of Central Intelligence, and other officers of the U.S. Government, as appropriate. The Task Force is to ensure that, to the maximum extent permitted by law, Federal agencies coordinate programs to accomplish the following: (1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and (2) locate, detain, prosecute, or deport any such aliens already present in the United States.
HSPD-3
Homeland Security Advisory System, March 11, 2002, establishes policy for the creation of a Homeland Security Advisory System, which shall provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. Establishes that the system will provide warnings in the form of a set of graduated "Threat Conditions" that will increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies will implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert.
HSPD-4
National Strategy to Combat Weapons of Mass Destruction, December 2002, sets forth the National Strategy to Combat Weapons of Mass Destruction based on three principal pillars: (1) Counterproliferation to Combat WMD Use, (2) Strengthened Nonproliferation to Combat WMD Proliferation, and (3) Consequence Management to Respond to WMD Use. The three pillars of the U.S. national strategy to combat WMD are seamless elements of a comprehensive approach. Serving to integrate the pillars are four cross-cutting enabling functions that need to be pursued on a priority basis: intelligence collection and analysis on WMD, delivery systems, and related technologies; research and development to improve our ability to address devolving threats; bilateral and multilateral cooperation; and targeted strategies against hostile states and terrorists.
HSPD-5
Management of Domestic Incidents, February 28, 2003, is intended to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system. In HSPD-5, the President designates the Secretary of Homeland Security as the Principal Federal Official for domestic incident management and empowers the Secretary to coordinate Federal resources used in response to or recovery from terrorist attacks, major disasters, or other emergencies in specific cases. The directive assigns specific responsibilities to the Attorney General, Secretary of Defense, Secretary of State, and the Assistants to the President for Homeland Security and National Security Affairs, and directs the heads of all Federal departments and agencies to provide their "full and prompt cooperation, resources, and support," as appropriate and consistent with their own responsibilities for protecting national security, to the Secretary of Homeland Security, Attorney General, Secretary of Defense, and Secretary of State in the exercise of leadership responsibilities and missions assigned in HSPD-5. The directive also notes that it does not alter, or impede the ability to carry out, the authorities of Federal departments and agencies to perform their responsibilities under law.
HSPD-6
Integration and Use of Screening Information, September 16, 2003, establishes the national policy to: (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information, as appropriate and to the full extent permitted by law, to support: (a) Federal, State, Territorial, local, tribal, foreign government, and private sector screening processes; and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.
HSPD-7
Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003, establishes a national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks.
HSPD-8
National Preparedness, December 17, 2003, establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen the preparedness capabilities of Federal, State, and local entities.
HSPD-9
Defense of United States Agriculture and Food, January 30, 2004, establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.
HSPD-10
Biodefense for the 21st Century, April 28, 2004, provides a comprehensive framework for the Nation's biodefense and, among other items, delineates the roles and responsibilities of Federal agencies and departments in continuing their efforts in this area.
HSPD-11
Comprehensive Terrorist-Related Screening Procedures, August 27, 2004, requires creation of a strategy and implementation plan for a coordinated and comprehensive approach to terrorist screening in order to improve and expand procedures to screen people, cargo, conveyances, and other entities and objects that pose a threat.
HSPD-12
Policy for a Common Identification for Federal Employees and Contractors, August 27, 2004, establishes a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. The resulting mandatory standard was issued by the National Institute for Standards and Technology as the Federal Information Processing Standards Publication.

Appendix D: Selected Federal Laws With a Nexus to Terrorism and Granting the FBI Jurisdiction to Investigate the Attendant Criminal Activity

10 U.S.C. 382
Emergency situations involving chemical or biological weapons of mass destruction (WMDs).
18 U.S.C. 175-178
Commonly known as the Biological Weapons Anti-Terrorism Act (BWAT), this act makes it unlawful for any person to knowingly develop, produce, stockpile, transfer, acquire, retain, or possess a biological agent, toxin, or delivery system for use as a weapon.
18 U.S.C. 229
Chemical Weapons Convention Implementation Act of 1998 (CWC) makes it unlawful for any person to knowingly develop, produce, or otherwise acquire, transfer (directly or indirectly), receive, stockpile, own, possess, or use or threaten to use any chemical weapon. This applies to all toxic chemicals, not just those listed on the CWC list.
18 U.S.C. 831
Makes it unlawful to intentionally receive, possess, use, transfer, alter, dispose of, or disperse any nuclear material or nuclear byproduct.
18 U.S.C. 1038
Referred to as the Stop Terrorist and Military Hoaxes Act, makes it unlawful for individuals to engage in any conduct with the intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of various terrorist-related statutes.
18 U.S.C. 2332a
Makes it unlawful for any person to use, threaten, or attempt or conspire to use a weapon of mass destruction, including any biological agent, toxin, or vector. Defines "weapon of mass destruction" to mean: (1) any destructive device with an explosive charge of more than four ounces; (2) any weapon that is designated or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; (3) any weapon involving a disease or organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Appendix E: 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, Chelan County, WA

Scana Corporation

South Carolina Public Service (Santee-Cooper)

Southern California Edison

Southern Company Generation

TransCanada

United States Society on Dams

Xcel Energy Corporation

Appendix F: 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, Risk Management Division

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 the Dam Safety Offices of:

- California
- Colorado
- Nebraska
- New Jersey
- Ohio
- Pennsylvania
- Virginia
- Washington

Appendix G: Acronyms and Abbreviations

ASDSO	Association of State Dam Safety Officials
BIA	Bureau of Indian Affairs
CCTV	Closed-Circuit Television
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOI	U.S. Department of the Interior
DOL	U.S. Department of Labor
EAP	Emergency Action Plan
EO	Executive Order
EPA	U.S. Environmental Protection Agency
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FOUO	For Official Use Only
FR	Federal Register
GCC	Government Coordinating Council
GW	Gigawatt
HAZMAT	Hazardous Materials
HHS	U.S. Department of Health and Human Services
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilating, and Air Conditioning
IBWC	International Boundary Water Commission
ICODS	Interagency Committee on Dam Safety
IDS	Intrusion Detection System
IFIP	Interagency Forum on Infrastructure Protection
JTTF	Joint Terrorism Task Force
MSHA	Mine Safety and Health Administration Act
MW	Megawatt
NDSRB	National Dam Safety Review Board
NHA	National Hydropower Association
NICC	National Infrastructure Coordinating Center
NID	National Inventory of Dams
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
NPS	National Park Service
NWRA	National Water Resources Association
OSM	Office of Surface Mining
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
R&D	Research and Development
RRP	Rapid Recovery Plan

(continued from previous page.)

SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SMCRA	Surface Mining Control and Reclamation Act
SPP	Security and Prosperity Partnership of North America
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
SSSP	Site-Specific Security Plan
TREAS	U.S. Department of the Treasury
TVA	Tennessee Valley Authority
USACE	U.S. Army Corps of Engineers
U.S.C.	United States Code
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
USSD	United States Society on Dams
VBIED	Vehicle-Borne Improvised Explosive Device
WMD	Weapons of Mass Destruction

Appendix H: Bibliography

Association of State Dam Safety Officials (www.damsafety.org).

Centers for Disease Control and Prevention (www.cdc.gov).

Centers for Disease Control and Prevention, Agency for Toxic Substances and Disease Registry (www.atsdr.cdc.gov).

Congressional Research Service, "*Terrorism and Security Issues Facing the Water Infrastructure Sector*," February 7, 2002 (http://carper.senate.gov/acrobat%20files/RS21026.pdf).

Defense Intelligence College, Counterterrorism Analysis Course, Introduction to Terrorist Intelligence Analysis, Part 2: Pre-Incident Indicators (www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm).

Federal Bureau of Investigation (www.fbi.gov).

Federal Bureau of Investigation, "*Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment*" (www.aiche.org/uploadedFiles/CCPS/Resources/fbi_wmd.pdf). This document includes a list of chemical/biological materials likely to be used in the furtherance of weapons of mass destruction terrorist activities.

Federal Dam Safety and Security Act of 2002, Public Law 104 303.

Federal Emergency Management Agency, Interagency Committee on Dam Safety, Federal Guidelines for Dam Safety: Selecting and Accommodating Inflow Design Floods for Dams, FEMA 93, June 1979 (reprinted April 2004) (www.dlr.enr.state.nc.us/images/fema-64.pdf).

Federal Emergency Management Agency, National Dam Safety Program, "*Plan Ahead for a Dam Failure*," updated December 13, 2006 (www.fema.gov/plan/prevent/damfailure/index.shtm).

Federal Energy Regulatory Commission, on hydropower (www.ferc.gov/industries/hydropower/gen-info.asp).

Federal Energy Regulatory Commission, Division of Dam Safety and Inspections Operating Manual (www.ferc.gov/industries/hydropower/safety/guidelines/ops-manual.pdf).

Federal Energy Regulatory Commission, Engineering Guidelines for the Evaluation of Hydropower Projects (updated January 25, 2005), www.ferc.gov/industries/hydropower/safety/guidelines/eng-guide.asp#skipnavsub).

Federal Energy Regulatory Commission, Security Program for Hydropower Projects (updated November 15, 2002) (www.ferc.gov/industries/hydropower/safety/guidelines/security.asp).

HowStuffWorks.com, "How Hydropower Plants Work, The Power of Water" (http://people.howstuffworks.com/hydropower-plant1.htm).

Kentucky State Police, Counter-Terrorism, "Threats Involving Weapons of Mass Destruction (WMD) and Emergency Actions, Potential Indicators of WMD Threats or Incidents" (www.kentuckystatepolice.org/terror.htm). This site lists several indicators, protective measures, and emergency procedures.

National Hydropower Association (www.hydro.org).

North Dakota Wing, Civil Air Patrol, "Terrorist Attack Indicators" (www.ndcap.org/downloads/terrorist_attack_indicators.doc).

Princeton University, Department of Public Safety, "What Is a 'Heightened Security State of Alert'?" (undated) (http://web.princeton.edu/sites/publicsafety/Documents/Alert_HeightenedAwareness_021203.doc).

Stanford University, Department of Civil and Environmental Engineering, National Performance of Dams Program (http://npdp.stanford.edu/index.html).

The White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003 (www.whitehouse.gov/pcipb/physical.html).

United States Society on Dams (www.ussdams.org).

U.S. Army Corps of Engineers (www.usace.army.mil).

U.S. Army Corps of Engineers, Hydroelectric Design Center (https://www.nwp.usace.army.mil/hdc).

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

U.S. Department of Commerce, Bureau of Industry and Security (www.bis.doc.gov).

U.S. Department of Homeland Security (www.dhs.gov/dhspublic/index.jsp).

U.S. Department of Homeland Security, "Potential Indicators of Threats Involving Vehicle-Borne Improvised Explosive Devices (VBIEDs)," Homeland Security Information Bulletin, May 15, 2003. This document includes a table of chemicals and other demolition paraphernalia used in recent truck bomb attacks against U.S. facilities.

U.S. Department of Homeland Security, Sector-Specific Plan: Dams as a Key Resource for Critical Infrastructure Protection, 2006.

Department of Homeland Security, Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff. This 3-day course can be sponsored by the States or asset owners and operators. Contact: Shawn O'Reilly, shawn.oreilly@dhs.gov, 703-235-5754; or Dennis Sill, dr.sill@dhs.gov, 703-235-5779.

U.S. Department of the Interior, Bureau of Reclamation, Dam Safety Office, "Dam Safety Overview" (www.usbr.gov/ssle/dam_safety/index.html).

U.S. Department of the Interior, Bureau of Reclamation, Teton Basin Project (www.usbr.gov/dataweb/html/teton1.html).

Utah State University at Logan, College of Engineering, Utah Water Research Laboratory, Institute for Dam Safety Risk Management, 2003 (www.engineering.usu.edu/uwrl/idsrm.htm).

West Virginia State Archives, "Buffalo Creek Disaster" (www.wvculture.org/history/buffcreek/bctitle.html).

Homeland Security

For Official Use Only (FOUO)