Assessment of the Bureau of Reclamation's Security Program

Committee to Assess the Bureau of Reclamationâ€™s Security Program, National Research Council

ISBN: 0-309-12528-6, 146 pages, 6x9, (2008)

ASSESSMENT OF THE BUREAU OF RECLAMATION'S SECURITY PROGRAM

Committee on the Assessment of the
Bureau of Reclamation's Security Program

Board on Infrastructure and the Constructed Environment
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract/Grant No. 05CS811164 between the National Academy of Sciences and the U.S. Bureau of Reclamation. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-12527-7
International Standard Book Number-10: 0-309-12527-8

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Cover photographs from top to bottom: Glen Canyon Dam (from the Committee on the Assessment of the Bureau of Reclamation's Security Program); Hoover Dam at night (from U.S. Bureau of Reclamation); Grand Coulee Dam (from the Committee on the Assessment of the Bureau of Reclamation's Security Program); Friant Dam (from U.S. Bureau of Reclamation); Folsom Dam (from U.S. Bureau of Reclamation)

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON THE ASSESSMENT OF THE BUREAU OF RECLAMATION'S SECURITY PROGRAM

JOHN T. CHRISTIAN, *Chair*, Consulting Engineer, Waban, Massachusetts
BILAL M. AYYUB, University of Maryland, College Park
GEORGE H. BAKER III, James Madison University, Harrisonburg, Virginia
DWIGHT A. BERANEK, Michael Baker, Jr., Inc., Alexandria, Virginia
MARK M. HANKEWYCZ, The Protection Engineering Group PC, Chantilly, Virginia
JEREMY ISENBERG, Weidlinger Associates, Inc. (retired), Atherton, California
L. MICHAEL KAAS, U.S. Department of the Interior (retired), Arlington, Virginia
DAVID A. KLINGER, University of Missouri, St. Louis
RICHARD G. LITTLE, University of Southern California, Los Angeles
JOHN A. McCARTHY, Kamal Advisory Services LLC, Dubai
CHARLES I. McGINNIS, U.S. Army Corps of Engineers (retired), Charlottesville, Virginia
KARLENE H. ROBERTS, University of California, Berkeley
RANDY ROSSMAN, Miami-Dade Police Department, Miami, Florida
CRAIG D. UCHIDA, Justice & Security Strategies, Silver Spring, Maryland

Staff

LYNDA STANLEY, Director
KEVIN LEWIS, Senior Program Officer
DANA CAINES, Financial Associate

Preface

Malicious acts intended to cause the failure of a major dam or dams are a threat to the nation and its citizens. Nearly 7 years ago, on September 11, 2001, 19 determined individuals took control of four airplanes with hundreds of passengers aboard and crashed the planes into the World Trade Center in New York City, the Pentagon in Washington, D.C., and a field in Pennsylvania, all within a matter of hours. In seeking to determine how these attacks could have happened, the 9/11 Commission found that the lack of preparedness was the result of an underlying "lack of imagination" on the part of the U.S. security enterprise. The commission concluded that although the 9/11 attacks were a shock, they should not have come as a surprise.

It is tempting to assume that, because no dams have yet been compromised by international terrorists or domestic extremists, it cannot someday happen. In the United States today more than 79,500 dams are used to control flooding and provide power and water for a variety of uses, and many would become significant hazards if they should fail. Some hold back millions of gallons of water, which, if unleashed in an uncontrolled way, could rush downstream and destroy lives, property, and communities.

Thirty-two years ago, the failure of the Teton Dam changed how the nation managed, inspected, and invested in dams. Following the 9/11 attacks, the physical assurance of dams took on new importance. Now the owners and operators of dams find they need to change the ways they identify threats to and vulnerabilities of dams, manage risk, and imple-

ment measures to protect dams from security-related failures. The owners and operators of large dams, including the U.S. Bureau of Reclamation, the U.S. Army Corps of Engineers, the Tennessee Valley Authority, and others, have recognized the potential consequences of an intentionally caused dam failure. They are consequently redefining their concept of stewardship and responsibility for their infrastructure to include physical security.

At the request of the U.S. Bureau of Reclamation, the National Research Council (NRC) appointed a multidisciplinary committee of 14 experts to assess Reclamation's security program and determine its level of preparedness to deter, respond to, and recover from malicious threats to its physical infrastructure and to the people who use and manage it. The committee held four meetings, and subgroups of committee members and NRC staff visited all five of Reclamation's regions and the Hoover, Shasta, Folsom, Glen Canyon, and Grand Coulee dams, among others. The committee held briefings and discussions with Reclamation's senior executives, program managers, regional directors, and area staff; Reclamation contractors and partners; and representatives of other federal agencies involved in dam security. The committee appreciates the exceptional cooperation, support, and insights provided by all of the Reclamation staff with whom it met. The committee also appreciates the support and insights of Reclamation's partners and its fellow federal agencies.

The committee's report is organized into five chapters. Chapter 1, "Context," describes Reclamation's security challenges, the history of its security program, previous reviews of that program, and the committee's approach for addressing the statement of task.

Chapter 2, "Description of Reclamation's Security Program," describes the program's organizational structure, the major responsibilities of the security, law enforcement, and emergency management offices, and the resources available to implement security-related activities.

Chapter 3, "Assessment of Reclamation's Security-Related Processes," contains the committee's observations and findings on Reclamation's physical security, law enforcement, and incident response processes, functions, and expertise, its organizational structure, and its working relationships.

Chapter 4, "Future Plans," contains the committee's observations and findings on the development of a robust, sustainable security program.

Chapter 5, "Conclusions and Recommendations," contains the committee's conclusions and its recommendations for improvement based on its observations and findings.

Although this report focuses on the Bureau of Reclamation, the security-related challenges described are not unique to that organization. Other owners and operators of large dams, including the U.S. Army

Corps of Engineers, the Tennessee Valley Authority, other federal agencies, states and localities, water and power authorities, and private-sector corporations, must grapple with similar challenges and find ways to meet them. Each of these organizations has its own history, culture, organizational structure, and physical location. The committee did not extend its investigations to consider security issues beyond the Bureau of Reclamation because time and resources were limited and because its mandate and authority extended only to the Bureau of Reclamation. Nevertheless, it believes that the nation would benefit from cooperation among the dam-owning organizations to ensure the security of their dams and the safety of the public. The public and private effort to develop guidelines and tools for protecting the nation's dams being led by the Department of Homeland Security is one way of doing this. Indeed it may be that a comprehensive review of the security of the nation's dams is called for. The committee hopes this report will contribute not only to the continued development of Reclamation's security program but also to the national dialogue on how best to ensure the physical security of the nation's dams and the people who rely on them for water and power.

John T. Christian, *Chair*
Committee on the Assessment of the
Bureau of Reclamation's Security Program

Acknowledgments

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Shawn Fenn, Ecology and the Environment Inc.,
James Fetzer, James Fetzer & Associates, LLC,
Gerald E. Galloway, Jr., University of Maryland,
Henry J. Hatch, U.S. Army Corps of Engineers (retired),
Michael Hightower, Sandia National Laboratories,
James H. Lambert, University of Virginia, and
Terrence P. Ryan, CPP, Raytheon.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by M. Granger

Morgan, Carnegie Mellon University. Appointed by the NRC, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

The committee also acknowledges and appreciates the contribution of the members of the Board on Infrastructure and the Constructed Environment (BICE) of the NRC. BICE was established in 1946 as the Building Research Advisory Board. It brings together experts from a wide range of scientific, engineering, and social science disciplines to discuss potential studies of interest, develop and frame study tasks, ensure proper project planning, suggest possible reviewers for reports produced by fully independent ad hoc study committees, and convene meetings to examine strategic issues. The board members were not asked to endorse the committee's conclusions or recommendations or to review the final draft of the report before its release.

Contents

Acronyms

ASCE	American Society of Civil Engineers
BLM	Bureau of Land Management
BOR	Bureau of Reclamation
CAPRA	Critical Asset and Portfolio Risk Analysis
CFR	comprehensive facility review
CIO	chief information officer
COOP	continuity of operations plan
CSR	comprehensive security review
DHS	Department of Homeland Security
DOI	Department of the Interior
DTRA	Defense Threat Reduction Agency
EAP	emergency action plan
ECQ	executive core qualification
EOC	emergency operations center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOUO	for official use only
FPS	Federal Protective Service

HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
ICS	incident command system
IED	improvised explosive device
IMARS	Incident Management and Reporting System
JTTF	Joint Terrorism Task Force
LEA	law enforcement administrator
MC	mission critical
MMC	major mission critical
MOU	memorandum of understanding
MSRA	Matrix Security Risk Assessment
NCI	national critical infrastructure
NEP	National Exercise Program
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NRC	National Research Council
NRF	National Response Framework
NRP	National Response Plan
OLESEM	Office of Law Enforcement, Security, and Emergency Management
OMB	Office of Management and Budget
OVI	occurrence, vulnerability, importance
PART	Program Assessment Rating Tool
PE	project essential
PEMO	Program and Emergency Management Office
PFR	periodic facility review
PIV	personal identity verification
PSR	periodic security review
RAM–D	Risk Assessment Methodology–Dams
RSA	regional special agent
RSO	regional security officer
SAT	security advisory team
SCADA	supervisory control and data analysis

SSLE	Security, Safety, and Law Enforcement
TSC	Technical Services Center
USACE	U.S. Army Corps of Engineers

Summary

One lesson from the September 11, 2001, attacks on the World Trade Center and the Pentagon is that infrastructure built for beneficial purposes can become an instrument of mass destruction if it fails as the result of a malicious act.[1] Dams and their related infrastructure are primarily built to control the flow of a river and mitigate flooding. The water impounded behind a dam can be used to generate power and to provide water for drinking, irrigation, commerce, industry, and recreation. However, if a dam fails,[2] the water that would be unleashed has the energy and power to cause mass destruction downstream, killing and injuring people and destroying property, agriculture, industry, and local and regional economies.

The significance of dams as vehicles of mass destruction has not gone unrecognized. Serbian forces attempted to blow up the Peruća dam in Croatia in 1993 during the Serbo-Croatian War. Hoover Dam was identified as a potential target for enemy forces during World War II, and the sabotage of Glen Canyon Dam was fictionalized in the 1975 novel *The Monkey Wrench Gang*.

[1]A malicious act is defined as a willful act of destruction perpetrated by a determined individual or group of individuals, such as international terrorists, domestic extremists, or a disgruntled employee.

[2]In this report, a dam failure is defined as the uncontrolled release of water from a reservoir such that lives and properties downstream are threatened. Various mechanisms can cause a dam failure.

The U.S. Bureau of Reclamation (hereinafter Reclamation or BOR) is responsible for managing and operating some of this nation's largest and most critical dams, including five national critical infrastructure (NCI) facilities:[3] the Hoover, Grand Coulee, Folsom, Shasta, and Glen Canyon dams. Reclamation's total inventory includes 249 facilities comprising 479 dams and dikes and related facilities. The importance of the water and power supplies provided by these facilities to the quality of life in 17 western states[4] cannot be overstated. The failure of one or more of these dams as the result of a malicious act would come with little warning and time for evacuation. In the worst case, where a large dam is located above a major population center, the devastation in terms of lost lives and destruction of property, power and water supply facilities, and commerce could rival or exceed that in New Orleans after the levees failed following Hurricane Katrina.

RECLAMATION'S SECURITY CHALLENGES

Reclamation's mission is to "manage, develop, and protect water and related resources in an environmentally and economically sound manner in the interest of the American public" (USBR, 2007). Major disruptions to its operations—the cutting off of water and power for days, weeks, or months—would have significant impacts on local and regional economies and on the lives of millions of people. Reclamation's overall security challenge, then, is to ensure the physical integrity of its facilities and the reliability of its power and water supplies if faced with a terrorist or other malicious act.

This challenge has multiple aspects, some of which involve balancing security with other societal objectives. For instance, Reclamation must find ways to allow public access to its facilities and services while limiting access to some on-site areas. It must identify vulnerabilities in its facilities and find ways to mitigate them. When an incident occurs, Reclamation must be prepared to respond rapidly and appropriately whether that facility is near a city or in a remote area. Reclamation must

[3]The National Infrastructure Protection Plan (NIPP) defines critical infrastructure as "assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters" (DHS, 2006, p. 103).

[4]Arizona, California, Colorado, Idaho, Kansas, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Texas, Utah, Washington, and Wyoming.

ensure that its staff, its operators,[5] its contractors,[6] and its stakeholders[7] do not include individuals who present a security threat. Finally, Reclamation must understand how risks and vulnerabilities might change in a world where new security threats are continually emerging.

In the nearly 7 years since the 9/11 attacks, Reclamation has invested significant resources—staff time and expertise, outside expertise, technical and physical measures, and funds—to establish and build a security program. It has completed threat and vulnerability assessments for most of its facilities; contracted for security guards and law enforcement officers; installed surveillance systems and physical barriers to protect against unauthorized intrusions; upgraded control systems; and conducted training exercises. Funding for these improvements has been primarily redirected to security from other Reclamation programs. Reclamation is now at a point where it is appropriate to evaluate the results of these efforts and determine how best to move forward to develop a security program that is robust and sustainable.

OVERVIEW OF THIS STUDY

At the request of the U.S. Bureau of Reclamation, the National Research Council, through the Board on Infrastructure and the Constructed Environment, appointed a multidisciplinary committee of 14 experts to assess Reclamation's security program and determine its level of preparedness to deter, respond to, and recover from malicious acts to its physical infrastructure and to the people who use and manage it.[8] The committee members have experience in government, academia, and the private sector and expertise in physical security, law enforcement, threat assessment and mitigation, risk analysis, dam safety, civil engineering, and emergency response (Appendix A).

---

[5]Operators: BOR dams and related facilities are operated either by BOR employees or by employees of the water districts to which BOR has transferred that authority.

[6]Contractors: individuals or companies hired to provide services (e.g., construction, maintenance, protection) at BOR facilities. Some water districts operate and maintain BOR-owned dams and related facilities. They may also hire contractors to perform services. BOR sometimes also calls these water districts contractors.

[7]Stakeholders: BOR stakeholders include the direct beneficiaries of its programs, such as users of irrigation, municipal, and industrial water, and consumers of power generated at BOR dams.

[8]The committee's statement of task (as described in Chapter 1) and this study cover only the security program of the Bureau of Reclamation. Although there are many other owners and operators of large dams that must grapple with similar challenges and ways to address them, the committee could not expand its investigations beyond its given task. The committee does believe, however, that a comprehensive review of the security of the nation's dams would be of value.

To accomplish its task, the committee met as a whole four times between January and November 2007. It received briefings from the staff of Reclamation's Security, Safety, and Law Enforcement (SSLE) Office and program managers from the Office of the Chief Information Officer (CIO). Some of the briefings included information that was classified as secret or for official use only (FOUO). Groups of two or three committee members and NRC staff also visited Reclamation's five regions, several area offices, and a number of dam sites, including the five national critical infrastructure facilities. They interviewed BOR's area office managers, law enforcement and security personnel, and BOR contractors and operators and observed the customs and practices of Reclamation staff in the field. The committee also received briefings and held discussions with BOR senior executives and representatives of other federal agencies involved in dam security (Appendix B).

The committee formulated its conclusions, findings, and recommendations based on previous reviews of Reclamation's security program; information gathered through the briefings, site visits, and discussions; a review of reference materials and studies; and the committee members' own expertise and experience.

CONCLUSIONS

The committee's overall conclusion is that although the Bureau of Reclamation is better able today to protect its infrastructure and its people against malicious acts than it was 7 years ago, the security program is not yet mature, well-integrated, or appropriately supported at all levels of the organization.

To date, Reclamation has focused on tactical issues: developing a risk management approach; establishing security plans for each facility; staffing a security and law enforcement office; and developing an intelligence gathering and analysis capability. Still missing are policies and operational guidance for effective responses to security-related incidents; performance measures to support continual improvement; and a method for disseminating lessons learned. Also missing are the full support and commitment of senior executives and managers at all levels of the organization and adequate resources—staff, expertise, and funding—to develop a security program that is robust and sustainable.

It is now time for Reclamation to take a more strategic approach to its security program. One of its highest priorities should be the development of a vision and a plan to provide a path forward. The vision should explicitly link the physical assurance of Reclamation's facilities to its overall mission of providing water and power. The plan should address policy, programmatic, and resource issues and should have the support and commitment of all of Reclamation's managers.

FINDINGS AND RECOMMENDATIONS

The committee's findings and recommendations follow. The recommendations are intentionally general to allow Reclamation and its SSLE Office some flexibility in determining what processes, tools, or policies will be used to address them. In some cases a recommendation relates to more than one finding.

With the exception of the development of a vision and a plan for the security program, the committee has not presented its recommendations in order of priority. However, some recommendations require action sooner than others because they will help to avoid undesirable outcomes and will yield both immediate and long-term benefits. These actions include the development of

- An out-of-cycle process for security assessments;
- Policy on the use of deadly force;
- Response plans for security-related incidents;
- A streamlined personal identity verification process;
- Preproject planning for security-related projects; and
- Procedures related to the sharing of intelligence-based information.

A Risk Management Approach

Finding 1: The risk management process that Reclamation has developed to assign priority for conducting threat and vulnerability assessments, security improvements, and resource allocation is appropriate. Elements of this process, however, need to be continually improved and refined as threats emerge, as risk assessment methods evolve, and as research-based information becomes available.

Recommendation 1: Reclamation managers should monitor the new threat and risk assessment methods being developed by the Department of Homeland Security and others and use those methods that are most appropriate for dams and related infrastructure (Finding 1).

Finding 2: Reclamation plans to conduct security assessments on a 3- to 6-year cycle even though security threats are continually emerging and must be continuously monitored.

Recommendation 2: In addition to conducting security assessments on a 3- to 6-year cycle, Reclamation should institute a process and criteria for conducting out-of-cycle assessments as threats emerge and circumstances warrant (Finding 2).

An Integrated Security Plan for Each Facility

Finding 3: A robust facility security plan provides for defense in depth through an integrated system made up of obstacles that restrict access, surveillance and intrusion detection systems, and a rapid-response force. Although elements of a facility security plan were visible at most sites that the committee visited, the elements did not appear to be effectively integrated.

Finding 4: At some sites, the committee could imagine threat scenarios, especially those involving insiders, that could not be countered effectively by the forces and fortifications in place. Too often facility security defenses appeared brittle and lacking in depth. If one line of facility security was neutralized, it was too likely that intruders could continue moving forward.

Finding 5: Reclamation evaluated a very limited number of standard threat scenarios for its security assessments. Security-related intelligence has not been integrated into site-specific, realistic threat scenarios to the committee's knowledge.

Recommendation 3: Reclamation and the SSLE should review their facility security plans as a system, identify gaps in the integration of the various elements, develop a range of realistic, site-specific threat scenarios based on local conditions and intelligence from all available sources, and conduct both contingency planning and training exercises using these scenarios. A protocol for regular review and adjustment of scenarios should be adopted to assure that planning and training are aligned with current conditions (Findings 3, 4, 5).

Finding 6: Because each Reclamation facility is in a different jurisdiction with different laws and a unique mix of local, county, state, and federal law enforcement entities, the interface between first responders and those that provide follow-up will vary. Facility security plans will therefore need to incorporate distinct arrangements for cooperation among the various responders during a security-related incident.

Finding 7: Specific guidelines for command, control, and decision making at individual sites enable an effective response to a security-related incident. At Reclamation, guidance for these responsibilities was unclear, and procedures were not well understood by staff.

Finding 8: Training exercises are important to ensure that when personnel from multiple government and law enforcement entities respond to

a security-related incident, all of the key players understand the procedures for command and control and for the transfer of authority as events unfold. Training exercises need to be designed to test site-specific, realistic scenarios and to be aligned with the responsibilities of the responders.

Recommendation 4: Reclamation should ensure that all security and law enforcement entities that would respond to a security-related incident at one of its facilities have a clear understanding of the lines of authority, roles, and responsibilities outlined in the response plan. The various security and law enforcement entities at each facility should train together to practice the actions each entity would be responsible for in a realistic scenario (Findings 6, 7, 8).

Finding 9: Good communication is critical for an effective response to a security-related incident. The committee observed that some communication equipment and technologies used by Reclamation and other federal, state, and local law enforcement and security organizations were not interoperable and would hinder communication among responders.

Finding 10: Certain communication technologies used in rural areas are subject to failure caused by weather and related events and may not be reliable during a security-related incident.

Recommendation 5: Reclamation should ensure that its personnel have the appropriate equipment and skills to communicate with all other entities expected to respond to a security-related incident. It should validate the effectiveness of the communication methods through appropriate exercises and simulations and work to standardize communication approaches (Findings 9, 10).

Finding 11: The use of standard ammunition in some parts of some Reclamation facilities could substantially compromise the integrity of critical equipment. It was not clear if this was common knowledge throughout SSLE or among those security and law enforcement entities that would respond to a security-related incident.

Recommendation 6: Reclamation should investigate how nonlethal weapons and new technologies can be used effectively during a response to a security-related incident (Finding 11).

Finding 12: The committee observed design and installation flaws in several risk mitigation projects. The personnel at the relevant facilities clearly believed that such flaws could have been avoided if the SSLE staff had

sought their input during the planning process, before the projects were designed and installed.

Recommendation 7: Reclamation should establish an effective pre-project planning process to improve the design of risk mitigation projects, avoid rework, use available resources more effectively, and improve working relationships. The SSLE should ensure that representatives from the area offices and facility operators are involved early in the process when decisions are made about project scope and implementation strategy (Finding 12).

POLICIES AND OPERATIONAL GUIDANCE FOR KEY ASPECTS OF THE PROGRAM

Finding 13: The distinction between law enforcement and security within Reclamation is not clear, and the resulting ambiguity has raised issues regarding the use of deadly force during a security-related incident.

Recommendation 8: Reclamation and the SSLE should work with local law enforcement entities to expedite the development of clear, legally binding guidance on the use of deadly force. The guidance should clearly address how the defense-of-life rule might apply in specific types of security-related incidents (Finding 13).

Finding 14: Reclamation has not adequately addressed threats posed by insiders—Reclamation staff, facility operators, contractors—to override physical security components and take control of dam operations.

Recommendation 9: Reclamation should determine if there are ways to streamline the personal identity verification process for employees and contractors while ensuring that the process remains effective in identifying those who might pose a threat to security. Criteria and a program for conducting periodic security reviews for key Reclamation personnel should also be developed (Finding 14).

Finding 15: Reclamation-wide guidance on site access procedures for contractors and on safeguarding plans and drawings for construction projects has not been issued. In the absence of such guidance, some area offices have developed their own procedures.

Recommendation 10: Reclamation and the SSLE should move expeditiously to develop policies for site access for contractors and for the safeguarding of project plans and drawings. Policies should be for-

mulated in close collaboration with area and regional managers and should be flexible enough to distinguish among different situations (Finding 15).

Finding 16: The objectives and operating procedures for law enforcement are different from those for security. The legislation giving Reclamation law enforcement authority does not address issues of antiterrorism or security, nor does it permit Reclamation to directly hire its own law enforcement personnel.

Recommendation 11: Reclamation's senior executives and security managers should identify the gaps in their authority for creating an effective security program and, if necessary, seek authorizing legislation that will allow implementation of a more robust program (Finding 16).

A COLLABORATIVE OPERATING ENVIRONMENT

Finding 17: With its largely decentralized organizational structure and heavy reliance on partnerships and contractors, Reclamation is fundamentally dependent on collaboration within and among organizations to achieve its mission. Imposing a centralized security program on a culture that is accustomed to distributed program management and authority has resulted in tensions and ineffective working relationships between the SSLE staff in Denver and the staff of regional and area offices.

Finding 18: Sound working relationships are based on effective communications and trust. Managerial actions and the behavior of SSLE's Denver-based staff have in some cases created distrust among the regional and area office staff that is damaging to internal working relationships and that limits the effectiveness of the security program.

Recommendation 12: SSLE managers should recognize and respect the importance that regional and area staff attach to their working relationships with their operators, contractors, and local law enforcement personnel. SSLE should work through the regional directors and area office managers when developing risk-mitigation projects and other activities that require the input of local law enforcement personnel, operators, and other stakeholders. SSLE should also intensify its efforts to communicate the goals, methods, priorities, and budget constraints of the security program through face-to-face meetings with regional and area office managers. To be effective, communication should routinely be two way (Findings 17, 18).

Finding 19: An inflexible commitment to the need-to-know doctrine inhibits the sharing of intelligence-based information among SSLE staff in Denver, the regional special agents, and the area office personnel who might be in the best position to deter some threats and who would be the first responders to an incident.

Recommendation 13: SSLE staff should endeavor to find ways to better inform senior managers and field personnel about potential threats to facilities based on security-related intelligence. They should also communicate the constraints under which they operate, especially the restrictions on dissemination of intelligence-based information (Finding 19).

Finding 20: Field personnel and others who have reported potentially valuable information about suspicious activities to the SSLE in Denver only rarely receive feedback on how or if the information was used. As a consequence, some field personnel view security-related communication as a one-way street and are reluctant to report information about suspicious activities since their effort appears to have no effect.

Recommendation 14: When security-related information is collected at the local level and forwarded to the Denver office, the SSLE should provide feedback on the disposition of that information. It should at least acknowledge receipt of the information and encourage continued reporting of suspicious activities (Finding 20).

Finding 21: Although the SSLE's Denver-based staff may have the technical skills to carry out their job responsibilities, they have not in general displayed the communication, negotiation, and team-building skills needed for the sound working relationships that are critical to Reclamation.

Recommendation 15: Reclamation should provide the SSLE staff with additional training in communication, negotiation, and team-building skills (Finding 21).

Senior Management Support and Commitment

Finding 22: Creating an effective security program and a culture of security requires the dedicated support and commitment of Reclamation's managers at all levels of the organization. Currently, such support and commitment are uneven. Some managers clearly understand the link between Reclamation's mission and security, and they are spearheading efforts to implement effective security procedures and programs. Others

regard security as an unwelcome intrusion into other activities and resent the redirection of resources from other activities to security.

Finding 23: Building commitment and support for the security program is primarily the responsibility of Reclamation's senior executives—the commissioner, deputy commissioners, and regional directors and the director and program managers of the SSLE Office.

Recommendation 16: Reclamation's senior executives and SSLE personnel should clearly communicate the critical link between security and Reclamation's mission. Management must guard against sending the wrong signals to field personnel: that terrorism "can't happen here [in rural America]"; that field personnel and operators no longer need to be vigilant; or that threats no longer exist because some steps have been taken to improve the security of facilities (Findings 22, 23).

Adequate Resources

Finding 24: The resources—number of staff, expertise, funding—currently available for Reclamation's security program are not sufficient to operate and sustain an effective program.

Finding 25: Folsom Dam requires special consideration within the national critical infrastructure classification owing to the magnitude of the potential consequences of a security-related failure. The level of resources required for effective security is greater at Folsom than elsewhere.

Recommendation 17: High-level attention should be given to determining how to provide additional resources to support a more robust security program without compromising other activities that are critical to Reclamation's mission (Findings 24, 25).

Finding 26: Security improvements benefit the public at large and are not limited to a specific set of stakeholders. Reclamation's proposal to make some security-related costs fully reimbursable creates tension with its stakeholders. The safety of dams program, in which reimbursable project costs are split between Reclamation and its stakeholders, may serve as a model for developing criteria, a process, and a cost-sharing percentage for reimbursing the costs of some security-related operations and maintenance activities.

Recommendation 18: Where stakeholder reimbursements are sought for security-related operations and maintenance activities, the ratio that is

used for the safety of dams program—85 percent federal funding and 15 percent stakeholder funding—should be considered as the starting point (Finding 26).

Performance Measurement

Finding 27: Reclamation has developed some performance measures for evaluating the risk mitigation component of its site security program. Additional measures are needed to evaluate processes related to deterrence of and response to security-related incidents.

Recommendation 19: Reclamation should establish a set of performance measures for its security program elements to encourage continual improvement. Where appropriate, it should use measures developed by other federal programs that are active in law enforcement and intelligence gathering. Performance outcomes should be measurable, achievable, and consistent (Finding 27).

A Method for Disseminating Lessons Learned

Finding 28: Lessons-learned processes can be useful for sharing experience-based information in an organization and for continually improving organizational processes, knowledge, and standards. Sources of lessons learned include after-action reports from training exercises, other forms of simulation, and other organizations.

Finding 29: Reclamation's security program does not appear to have a formal lessons-learned program in place. Where after-action reports followed major exercises, they were not disseminated to all the regions or the area offices that could have benefited from knowing the exercise results.

Recommendation 20: In the short term, SSLE should distribute after-action reports to the appropriate staff at all area and regional offices to leverage the knowledge gained from training exercises. The field staff should ensure that the documents are kept secure. In the longer term, Reclamation should develop a process and a database for capturing and disseminating lessons learned by looking to other organizations and agencies that have successful lessons-learned approaches (Findings 28, 29).

A Vision and a Long-Term Plan

Finding 30: Among their other objectives, organizational mission and vision statements, plans, and goals are meant to inspire and motivate

employees and stakeholders. Typically, they are driven by an organization's senior executives and reflect their priorities and values. Infrastructure security does not appear explicitly in Reclamation's mission and vision statements, plans, or goals. The failure to mention it conveys the idea that infrastructure security does not have the support and commitment of senior management, nor has it been given priority.

Finding 31: Reclamation does not appear to have a plan for a security program that is robust, mature, and sustainable. When asked about their goals for the security program, senior managers focused on tactical issues. Strategic issues, such as how security is to be embedded in Reclamation's culture and how regional security coordination is to be improved, were not mentioned.

Recommendation 21: Where appropriate, Reclamation's leadership should emphasize in its policy statements the link between security and the achievement of Reclamation's mission. A plan for sustaining an effective security program should be developed. Such a plan should include a vision, goals, and objectives, and strategies for accomplishing them (Findings 30 and 31).

REFERENCES

Department of Homeland Security (DHS). 2006. *National Infrastructure Protection Plan*. Washington, D.C.: DHS. More information available at www.dhs.gov/nipp.

U.S. Bureau of Reclamation (BOR). 2007. "Mission statement." Available at www.usbr.gov/main/about/mission.html.

1

Context

One lesson from the September 11, 2001, attacks on the World Trade Center and the Pentagon is that buildings and infrastructure constructed for beneficial purposes can become instruments of mass destruction if they fail as the result of a malicious act.[1] Dams are primarily constructed for beneficial purposes: to control the flow of a river and mitigate flooding. The water impounded behind a dam can be used to generate power and to provide water for drinking, industry, irrigation, and recreation. However, the uncontrolled release of the wall of water behind a major dam can cause mass destruction to areas and communities downstream. Dam-failure-related disasters, while rare, have resulted in as many as 85,000 deaths (the Banquiao and Shimantan dams, China, 1975); the devastation of towns and infrastructure (South Fork Dam, Johnstown, Pennsylvania, 1889, and St. Francis Dam, Los Angeles, California, 1928); and hundreds of millions of dollars in damages (Teton Dam, Madison County, Idaho, 1976) (Table 1.1).

To date, no dam failure has been caused by a malicious act. However, the potential for dams to cause mass destruction has not gone unrecognized. Hoover Dam was identified as a potential target for enemy forces during World War II (Pfaff, 2003) and the sabotage of Glen Canyon Dam was fictionalized in the novel *The Monkey Wrench Gang* (Abbey and

[1]A malicious act is defined as a willful act of destruction perpetrated by a determined individual or group of individuals, such as international terrorists, domestic extremists, or a disgruntled employee.

TABLE 1.1 Some Dam Failures and Their Consequences

Dam	Year	Location	Failure Mode	Consequences
Ka Loko Reservoir	2006	Kauai, Hawaii	Unusually heavy rain	7 killed
Val di Stava	1985	Near Trento, Italy	Poor maintenance; failure of outlet pipes	268 killed; 62 buildings and 8 bridges destroyed
Lawn Lake and Cascade dams	1982	Rocky Mountain National Park	Poor maintenance; outlet pipe erosion	3 killed; $31 million in damage (1982 dollars)
Morvi Dam	1979	India	Excessive rain; massive flooding	15,000 killed
Kelly Barnes Dam	1977	Toccoa, Georgia	Combination of factors	39 killed; property damage in surrounding area
Teton Dam	1976	Idaho	Internal erosion as dam being filled	11 killed; several towns destroyed; $300 million in damages (1976 dollars)
Banquiao and Shimantan	1975	China	Extreme rainfall beyond design capability of dam	85,000 killed
Baldwin Hills Reservoir	1963	Los Angeles, California	Subsidence leading to cracking of asphalt impervious seal	5 killed, 277 homes destroyed
Vajont	1963	Italy	Tectonic failure	Est. 2,000 killed; several villages wrecked
Malpasset	1959	Côte d'Azur, France	Geological failure; rupture along foundation joints	421 killed; $68 million in damage (1959 dollars)
St. Francis Dam	1928	Los Angeles, California	Geological instability; human error; failure of left abutment	More than 450 killed; one power plant and other properties destroyed
Austin	1911	Potter County, Pennsylvania	Design flaws	78 killed; $10 million in damage (1911 dollars)
South Fork	1889	Johnstown, Pennsylvania	Poor maintenance; heavy rain	2,200 killed; several towns destroyed

Brinkley, 1975). Serbian forces attempted to blow up the Peruća Dam in Croatia in 1993 during the Serbo-Croatian War. The attempt was thwarted, preventing a disaster for people in the cities and towns downstream (Nonveiller et al., 1999).

Across the United States, 79,500 dams in operation today are more than 25 feet high and are considered to be significant hazards if they fail (FEMA, 2006). Some of the most significant and iconic of these are owned and managed by the U.S. Bureau of Reclamation (hereinafter BOR or Reclamation). BOR's mission is to manage, develop, and protect water and related resources in an environmentally and economically sound manner in the interest of the American public. This mission can be carried out only if Reclamation can secure its dams and related infrastructure from terrorist or other malicious acts.

RECLAMATION'S SECURITY CHALLENGES

The Bureau of Reclamation was established in 1902 to bring water to 17 western states.[2] The importance of the water and power produced by BOR to the quality of life in the West cannot be overstated. Today, Reclamation is the nation's largest wholesaler of water, serving more than 31 million people and several large cities, including Denver, Seattle, Salt Lake City, Sacramento, San Francisco, Los Angeles, Las Vegas, and Phoenix. It provides the water to irrigate 10 million acres of farmland, which, in turn, produce 60 percent of the nation's vegetables and one-quarter of its fruit and nut crops. It is the second largest producer of hydroelectric power in the western United States: 58 power plants annually provide more than 40 billion kilowatt-hours of electricity to heat, cool, light, and power homes, factories, businesses, and government facilities. Approximately 90 million people visit 300 recreation sites, including Lake Havasu, Lake Mead, and Lake Powell, each year.

Major disruptions to Reclamation's operations—the cutting off of water and power for days, weeks, or months—would have a significant impact on local and regional economies and on the lives of millions of people. Thus, Reclamation's overriding security challenge is to assure the physical integrity of its facilities and the reliability of its power and water supplies if faced with a terrorist or other malicious act.

Currently, Reclamation manages 249 facilities comprising 479 dams and dikes, including such iconic and massive structures as the Hoover, Grand Coulee, Glen Canyon, Shasta, and Folsom dams (Figure 1.1). These facilities are distributed across 17 states. Some dams are in remote areas

[2]Arizona, California, Colorado, Idaho, Kansas, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Texas, Utah, Washington, and Wyoming.

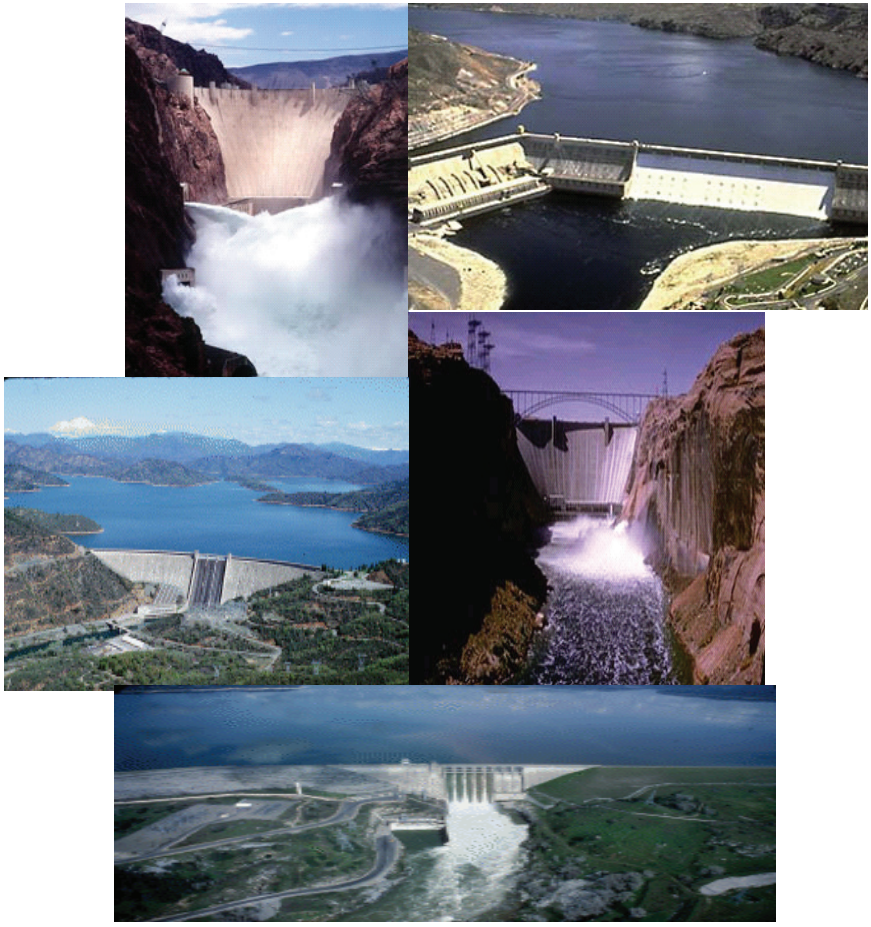


FIGURE 1.1 Hoover, Grand Coulee, Glen Canyon, Shasta, and Folsom dams. SOURCE: BOR Web site.

not easily accessed by air or by road. Others that were once in rural areas are now surrounded by cities and towns as a result of population growth and urban development. In some cases, service roads originally built across the tops of dams to provide access for operations and maintenance crews have been incorporated into key transportation corridors serving commuters and trucking.

Reclamation's security challenge has multiple aspects, including several that involve balancing security measures with other societal needs

and objectives. For example, Reclamation must find ways to provide public access to its facilities for transportation and recreation purposes and concurrently limit access to some areas within facilities. If an incident occurs, Reclamation must be prepared to respond rapidly and appropriately wherever the facility is located.

Reclamation must also identify vulnerabilities in its facilities and find ways to mitigate the risk that someone will exploit them. Each BOR facility is unique, although they share some common physical, human, and cyber elements. Most dam facilities comprise the dam itself, water impoundments or reservoirs, power plants, spillways, outlet works, penstocks (pipelines or conduits to turbines), and control rooms. However, the dams are built of different materials, have different configurations, and use different methods to impound water. The amount of water impounded by any single dam varies by season and weather condition. Each component and structure type potentially incorporates vulnerabilities that could be exploited. Reclamation needs not only to identify existing vulnerabilities but also to understand how they might change in a world where security threats are continually emerging.

In addition to protecting individual facilities, Reclamation must consider their interdependencies with other facilities. Many dams were built as interconnected components of systems to control major river basins and watersheds, such as the Colorado and Missouri river basins, the Central Valley Project in California, and the Columbia Basin Project in Washington. Although facilities along these watersheds are separated geographically, their operations are interconnected. Some are manned 24 hours per day, 7 days per week, while others are manned only part time or are controlled remotely through supervisory control and data analysis (SCADA) systems. Reclamation's facilities are in some cases interdependent with other infrastructure that is not under its direct control. Switchyards, roads, bridges, dams, and power plants owned or managed by other federal, state, or local organizations or by the private sector could, if compromised, damage Reclamation's facilities and their capacity to provide water and power. Mitigating such vulnerabilities requires BOR staff to partner with staff at other organizations such as the Department of Energy, the U.S. Army Corps of Engineers (USACE), and state departments of transportation.

The human elements of Reclamation's operations also present a security challenge. Its dams may be operated by federal government staff, local water and power authorities, or some combination of the two. Hundreds of contract workers access Reclamation's facilities every day to implement new construction or to carry out renovation, repair, and maintenance. BOR must ensure that its staff, its operators, and its contractors do not include individuals who present a security threat.

Finally, Reclamation is challenged to provide adequate resources—staff, funds, expertise—to conduct an effective security program while conducting its other programs and operations. In the last several years, Reclamation's overall budget has been decreasing even though the costs of maintaining and repairing existing infrastructure are rising for a number of reasons, among them the age of its facilities and increased stakeholder attention to environmental issues (NRC, 2006). The security program has been staffed and funded primarily by redirecting resources from other programs, placing additional constraints and pressures on Reclamation's budget.

TETON DAM FAILURE AND RECLAMATION'S RESPONSE

In its 105-year history, BOR has experienced one major dam failure, that of the Teton Dam in Madison County, Idaho (Figure 1.2).

Teton Dam was a 305-foot-high earth-filled dam constructed across the Teton River. The dam failed catastrophically and completely on June 5, 1976, just as it was being filled for the first time. The failure was initiated by a large leak about 130 feet below the crest of the dam. The first signs of the leak appeared at 7:30 a.m. By 8:00 p.m. the reservoir had emptied completely, triggering more than 200 landslides. The 30-foot-high wall of water released from the reservoir killed 11 people and destroyed entire downstream communities (Figure 1.3).

FIGURE 1.2 Teton Dam failure. View northwest toward the breach. The canyon floor is flooded from bank to bank, and all works there are completely inundated. SOURCE: BOR.

FIGURE 1.3 Teton Dam failure. Flood waters advancing through Rexburg, Idaho. SOURCE: BOR.

Although the federal response to the Teton Dam failure was immediate and far reaching, the costs were high. President Gerald Ford requested a $200 million appropriation to pay for damages. By 1987 more than 7,500 claims totaling more than $300 million had been paid.

The Teton Dam failure, followed by the Kelly Barnes Dam failure in 1977, changed how BOR and the nation managed, inspected, and invested in dams. Since 1976, Reclamation has institutionalized a rigorous review of every major dam under its purview under the congressionally authorized safety of dams program. That program requires a comprehensive facility review (CFR) every 6 years by subject-matter experts. A CFR includes a detailed dam inspection, identification of any change in loading on the dam or in downstream population and development, and a risk assessment. Periodic facility reviews (PFRs), which involve detailed inspections of dams, are performed midway between CFRs. Annual inspections are conducted by Reclamation's area offices in those years that CFRs or PFRs are not done. In addition to the dam safety aspects of the facility reviews and inspections, major operational and maintenance requirements are identified. Requests for funding to pay for such requirements are prioritized based on urgency and availability of funds.

Emergency action plans (EAPs) have been developed for all of Reclamation's dams. The plans are intended to lay out clearly the roles and responsibilities of BOR staff and others who would be called on to act in the event of a safety-related dam failure. By statute, Reclamation staff are

responsible for notifying local officials of an emergency. Local officials, in turn, are responsible for warning the general public and for setting evacuation plans in motion. EAPs are updated annually for all high dams that are a significant hazard. Training exercises are performed for each "high hazard dam" and "significant hazard dam" every 3 and 6 years, respectively. During these exercises the BOR staff and other responders practice a timed response to a simulated incident in order to test roles, responsibilities, and lines of communication.

In 1998, Reclamation established a "risk cadre," whose members were five experts at the Denver Technical Services Center (TSC)[3] assigned to further the risk analysis processes for dam safety. The risk cadre developed a consistent risk analysis methodology, developed toolboxes of methodologies for dam loading probability and consequences, and trained others in risk analysis, with the objective of continually improving the organization's risk analysis procedures.

BOR also works with other federal agencies in support of the Federal Emergency Management Agency (FEMA), which was directed to establish a national dam safety program under the Water Resources and Development Act of 1996. FEMA coordinates federal agencies' dam safety programs and promotes dam safety through state and local government organizations. FEMA's responsibilities were expanded by the Dam Safety and Security Act of 2002 (P.L. 107-310) to include developing technical assistance, materials, seminars, and guidelines to improve the security of U.S. dams.

Today, dam safety has matured into a well-established set of regulations, programs, and organizations. Reclamation's vision statement and goals clearly consider dam safety essential to its mission, and responsibility for dam safety is firmly embedded in its culture. And now, in the face of twenty-first century realities, Reclamation is challenged to proactively develop a security program and culture that are as robust as its program for dam safety.

HISTORY OF RECLAMATION'S SECURITY PROGRAM

Reclamation has recognized that terrorism and other malicious acts pose a threat to its facilities, its people, its customers, and the general public. In response to the 1995 bombing of the Alfred C. Murrah Building in Oklahoma City and the 9/11 attacks, Reclamation has invested significant resources—staff time and expertise, outside expertise, technical and physical measures, and funds—to build a security program. On November 12, 2001, Congress enacted P.L. 107-69, which provided Reclamation with law

[3]The TSC provides centralized engineering and scientific services that are typically beyond the capabilities of the areas and the regions (NRC, 2006). It is located in Denver.

enforcement authority at all of its facilities.[4] The law allows Reclamation to use law enforcement personnel from the Department of the Interior (DOI) or other federal agencies (except the Department of Defense). Reclamation may not itself directly hire law enforcement personnel. The BOR's Security, Safety, and Law Enforcement (SSLE) Office was subsequently established to focus on critical security needs. It was initially staffed by personnel from other BOR programs. One of SSLE's first activities was the development of a long-range strategy for comprehensive security risk assessments at all critical facilities. The safety of dams program was the model for assessing the security risk, decision making, and incident response procedures and programs.

In February 2003, Homeland Security Presidential Directive 5 (HSPD-5), Management of Domestic Incidents, was issued to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive National Incident Management System (NIMS). The objective of the directive is to ensure that all levels of government across the nation are able to work together efficiently and effectively in response to domestic incidents regardless of their cause, size, or complexity (EOP, 2003a). HSPD-5 also notes that

> initial responsibility for managing incidents generally falls on State and local authorities. The Federal government will assist State and local authorities when their resources are overwhelmed or when Federal interests are involved. The Secretary will coordinate with State and local governments to ensure adequate planning, equipment, training, and exercise activities. (EOP, 2003a, p. 1)

The Departmental Manual of DOI incorporates policy for the coordination of emergency management incidents, which include terrorist attacks and threats, floods, and other occurrences. The policy states that incident management activities must be initiated and conducted using the principles contained in the NIMS and that response activities are to be managed at the lowest possible organizational level (DOI, 2006).

In December 2003, Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, was issued. It established national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and protect them from terrorist attacks. The directive states as follows:

[4]The Bureau of Reclamation had no law enforcement authority with the exception of the police force at Hoover Dam before enactment of this law. Instead, BOR relied on support from other Department of Interior bureaus and from local law enforcement agencies that worked with specific BOR facilities.

> The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being. (EOP, 2003b, p. 1)

Under this directive, Reclamation and other federal agencies are required to

- Identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them;
- Work with state and local governments and the private sector to accomplish this objective;
- Ensure that homeland security programs do not diminish the overall economic security of the United States;
- Appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources;
- Conduct or facilitate vulnerability assessments of their infrastructure; and
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

In response to HSPD-7, the National Infrastructure Protection Plan (NIPP) was written and issued in 2006. It defines critical infrastructure as "assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety or any combination of those matters (NIPP, 2006, p. 103).[5] NIPP also outlines how the Department of Homeland Security (DHS) and its stakeholders will organize and carry out the national effort to protect 18 categories of infrastructure, including dams. It establishes national goals and objectives, introduces a risk-management framework that supports the national goals, and proposes key actions that are crucial to meeting the national goals.

[5]Five of Reclamation's dams are designated as national critical infrastructure.

DHS has also drafted a sector-specific plan[6] for the protection of dams and related resources. The plan sets out strategies for identifying dam assets, assessing vulnerabilities and prioritizing assets, developing protective programs, and planning for research and development. BOR helped to develop the dam sector plan in collaboration with USACE, other federal agencies, and other owners and operators of large dams (OMB, 2007).

In the 6 years after the 9/11 attacks, Reclamation

- Completed threat and vulnerability assessments for about 300 dams and related facilities;
- Hired security guards for its NCI dams and for some other critical facilities;
- Installed cameras and deployed other security measures such as barriers, bollards, fences, and gates to limit access to facilities;
- Closed or limited the use of some roads that traverse dams;
- Installed redundant control systems and upgraded SCADA systems for dams and related facilities; and
- Conducted internal training through seminars and tabletop and full-scale exercises. Special events, including the 2002 Winter Olympics, the 2002 BOR Centennial, and the 2004 Lewis and Clark Bicentennial, received additional security attention and provided opportunities for security training.

PREVIOUS REVIEWS OF RECLAMATION'S SECURITY PROGRAM

Early in its effort to establish a security program, Reclamation requested a top-down security program review to ensure that the program becomes balanced and sustainable and is based on a graded approach to protection.[7] The review was conducted by experts from Sandia National Laboratories and the Interagency Forum for Infrastructure Protection,[8] who collected data between July 29 and December 18, 2002. These outside experts were tasked to (1) evaluate the organizational structure, policies, and processes of BOR's security program and (2) make recommendations

[6]The report is designated For Official Use Only and is exempted from disclosure to the public.

[7]A graded approach gives the greatest of protection to the most important assets.

[8]The Interagency Forum on Infrastructure Protection included the Army Corps of Engineers, Tennessee Valley Authority, Bonneville Power Administration, Western Area Power Administrations, Federal Emergency Management Agency, Federal Energy Regulatory Commission, Sandia National Laboratories, Association of State Dam Safety Officials, and others.

for a mature, sustainable security program. The final report was issued in June 2003.[9]

The top-down review contained a series of recommendations for enhancing and sustaining the security program. It was adopted by Reclamation as the roadmap for long-term security policies and strategies. Many of the recommendations have been or are being implemented.

Two years later, in 2005, Reclamation's security program was reviewed by the Program Integrity Division of DOI's Office of the Inspector General. The review focused on whether Reclamation had implemented an adequate security program for its dams, particularly at the five NCI sites and other major dams, and whether funds appropriated for dam security had been properly expended.[10]

The performance of one element of Reclamation's security program, site security, was reviewed by the Office of Management and Budget (OMB) in 2005 and 2006. The OMB review is based on the Program Assessment Rating Tool (PART) that was developed to assess and improve the performance of federal government programs and achieve better results. The PART review is intended to identify a program's strengths and weaknesses to inform funding and management decisions aimed at making the program more effective. It looks at all factors that affect and reflect program performance, including program purpose and design; performance measurement, evaluations, and strategic planning; program management; and program results. The PART includes a consistent series of analytical questions that are intended to determine if programs are improving over time and to allow comparisons between similar programs in different agencies (OMB, 2007).[11]

OMB rated Reclamation's site security program as "moderately effective," which OMB defines as having set ambitious goals and being well managed. In summarizing its findings, OMB reported that

> the program has been re-invented since September 11, 2001, and after several rounds of internal and external reviews has made notable progress in improving the safety and security of key Reclamation facilities. To date it has made the most progress on upgrading the security of National Critical Infrastructure facilities, and is next moving to upgrade lower-risk facilities.
>
> The program has recently developed several creative and useful performance measures that will help track program accomplishments and

[9]The report is designated For Official Use Only and is exempted from disclosure to the public.

[10]The report is designated For Official Use Only and is exempted from disclosure to the public.

[11]OMB has also evaluated 13 other Reclamation programs, including the safety of dams program, which was given the highest rating, "effective."

> efficiency, but because they are new have not yet been used to guide program development or funding.
>
> Program oversight within the Department of the Interior falls outside normal program and budget pathways, possibly impairing internal program oversight. Also, certain oversight officials do not have the necessary security clearances, which limits their effectiveness and may cause internal information flow problems. (OMB, 2007, p. 1)

The report states that the OMB was taking action to (1) improve the linkage between program performance and program budget requests; (2) reexamine the internal management of the program to improve internal oversight and communication between BOR and DOI staff; and (3) collect performance information and refine timelines and cost estimates for reducing risk at critical and project-essential facilities.

STATEMENT OF TASK

At the request of the BOR, the NRC, through the Board on Infrastructure and the Constructed Environment, appointed a committee of 14 experts to assess BOR's security program and determine its preparedness to prevent, deter, respond to, and recover from malicious acts to BOR's physical infrastructure and to the people who use and manage it. The members of this multidisciplinary committee have broad and substantial experience and expertise in physical security, law enforcement, threat assessment and mitigation, risk analysis, dam safety, civil engineering, and emergency response. They have worked in government, academia, and the private sector.

To meet its charge, the committee was asked to:

> (1) Assess security, law enforcement, and emergency management response processes, functions, and expertise to determine whether the BOR is appropriately structured and has the required expertise to effectively protect its infrastructure and its people and assess the BOR's working relationships with other organizations involved with security and law enforcement functions, including other units within the Department of the Interior and other federal, state, and local agencies;
>
> (2) Evaluate BOR's future plans for its security, law enforcement, and emergency management programs;
>
> (3) Recommend strategies, methods, and practices to integrate security principles, policies, practices, and a culture of security throughout the organization, from headquarters to the field;
>
> (4) Develop a prioritized set of recommended actions that should be taken to close any gaps in preparedness or effectiveness.

The committee notes that the overarching statement refers to Reclamation's level of preparedness to "respond to . . . malicious acts," but that the individual tasks refer to emergency management response processes, functions, and expertise. In discussions and briefings with Reclamation and SSLE staff it was clear that the committee was being asked to evaluate how well prepared Reclamation is to respond to security-related incidents. Therefore, the committee's assessment focuses on Reclamation's processes, functions, and expertise for responding to security-related incidents.

The committee also notes that this report covers only the Bureau of Reclamation, although there are many other owners and operators of large dams in the United States, including USACE, the Tennessee Valley Authority, other federal agencies, states and localities, water and power authorities, and private sector corporations that must grapple with similar security challenges and find ways to overcome them. The committee could not extend its investigations beyond the security issues faced by the Bureau of Reclamation. It believes, however, that a comprehensive review of the security of the nation's dams would be of value.

THE COMMITTEE'S APPROACH

To accomplish its tasks, the committee met as a whole four times between January and November 2007. At the first two meetings, the committee received briefings from the SSLE's directors and program managers and from program managers in the office of the Chief Information Officer (CIO). Some of the briefings presented information that was classified as secret or sensitive. Groups of two or three committee members and NRC staff visited the BOR's five national critical infrastructure facilities and other dams. During the site visits, the committee members met with the senior staff at four regional offices—Salt Lake City, Utah; Sacramento, California; Boulder City, Nevada; and Boise, Idaho—and at several area offices, including Casper, Wyoming. The committee members also interviewed area office managers, law enforcement and security personnel, and BOR operators and contractors and observed the customs and practices of BOR staff in the field. After completing all the site visits, the groups met as the full committee to report on and discuss their observations and findings.

The committee also received briefings on the physical security of dams and BOR's security program from Reclamation representatives in Washington, D.C., and staff from DOI and discussed issues with both sets of individuals. To gain an outside perspective, the committee conducted a roundtable discussion with staff from the DHS, FEMA, and USACE about their dam-related security programs and security issues

in general. The committee's meetings, briefings, and site visits are listed in Appendix B.

To promote open and candid discussions throughout the study, the participants were assured that comments would not be attributed to specific individuals. Important facts and opinions were learned in this way and have been relied on for the development of this report.

The committee formulated its findings and recommendations on the basis of earlier reviews of BOR's security program, information gathered in the course of the briefings, site visits, and discussions, a review of reference materials and studies, and on the committee members' own expertise and experience.

REFERENCES

Abbey, Edward, and Douglas Brinkley. 1975. *The Monkey Wrench Gang.* First Edition. Philadelphia, Pa.: J.B. Lippincott Company.

Department of the Interior (DOI). 2006. *Departmental Manual.* Chapter 4: Coordination of Emergency Management Incidents. Available at http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3696.

Executive Office of the President (EOP). 2003a. *Homeland Security Presidential Directive 5, Management of Domestic Incidents.* Available at www.nimsonline.com/presidential_directives/hspd_5.htm.

EOP. 2003b. *Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization and Protection.* Available at www.fas.org/irp/offdocs/nspd/hspd-7.html.

Federal Emergency Management Agency (FEMA). 2006. *Dam Safety and Security in the U.S. A Report on the National Dam Safety Program.* Fiscal Years 2005 and 2006. FEMA 576. Available at www.fema.gov/library/viewRecord.do?id=2139.

Nonveiller, E., J. Rupcic, and Z. Sever. 1999. War damages and construction of Peruca Dam. *Journal of Geotechnical and Geoenvironmental Engineering* 125(4): 280-288.

Office of Management and Budget (OMB). 2007. *Program Assessment. Bureau of Reclamation—Site Security.* Available at www.whitehouse.gov/omb/expectmore/summary/10003701.2005.html.

Pfaff, Christine. 2003. "Safeguarding Hoover Dam during World War II." *The U.S. National Archives and Records Administration* Vol. 35. No. 2.

2

Description of Reclamation's Security Program

The Bureau of Reclamation (hereinafter Reclamation or BOR) is one of eight bureaus within the Department of the Interior (DOI)[1]. DOI's Office of Law Enforcement, Security and Emergency Management (OLESEM) is responsible for providing leadership, policy guidance, and oversight for law enforcement, homeland security, emergency management, and information security to each of the bureaus.

At Reclamation, the security program has several components: security, law enforcement, emergency management, and information and information technology (IT) security. All aspects of the security program are centrally managed through Reclamation's offices in Denver, Colorado, and Washington, D.C. The Security, Safety, and Law Enforcement (SSLE) Office manages the security, law enforcement, and emergency management components, while the information and IT security component is under the purview of the chief information officer (CIO). The director of SSLE reports to the deputy commissioner for policy, administration, and budget, while the CIO reports to the director of administration (Figure 2.1). The director of SSLE and the CIO are expected to work closely together to ensure the security of the supervisory control and data analysis (SCADA) systems used to operate dams, power plants, and related infrastructure and of other IT systems.

[1]The others are the Bureau of Indian Affairs; Bureau of Land Management; Fish and Wildlife Service; Minerals and Management Service; National Park Service; Office of Surface Mining; and the U.S. Geological Survey.

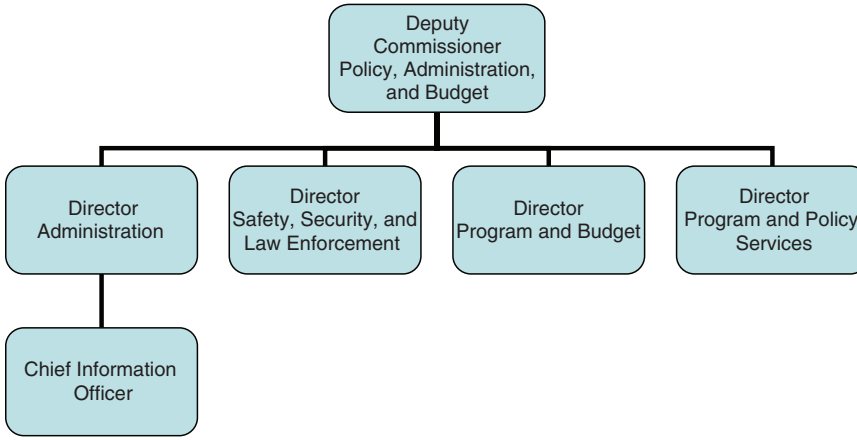


FIGURE 2.1 Reporting structures for SSLE and CIO.

The centralized management structure for security contrasts with the way most other BOR functions are managed. Since 1994, BOR has delegated much of its authority for program management and implementation to its 5 regional and 24 area offices (Figure 2.2). Authority formerly exercised from BOR central offices in Denver was delegated to lower organizational levels, and senior personnel positions at the central location were eliminated. At the same time, the Reclamation-wide directives known as *Instructions* were withdrawn. Mandatory requirements that replace the *Instructions* have been and continue to be developed and published as policy and directives in the *Reclamation Manual*, a Web-based collection of policies and directions that is continuously updated and revised[2] (NRC, 2006).

Reclamation's facilities are managed by the 24 area offices, with each of the five regional offices having full responsibility for operating and maintaining the assets in its region. In most but not all cases, this means that all the assets in a single watershed are operated and maintained by the same regional office. The exceptions include the Colorado, Canadian, and Rio Grande river basins, each of which needs an additional level of coordination (NRC, 2006).

Reclamation also oversees operations and maintenance activities where the responsibilities for implementing operations and maintenance

[2]Available at http://www.usbr.gov/recman.

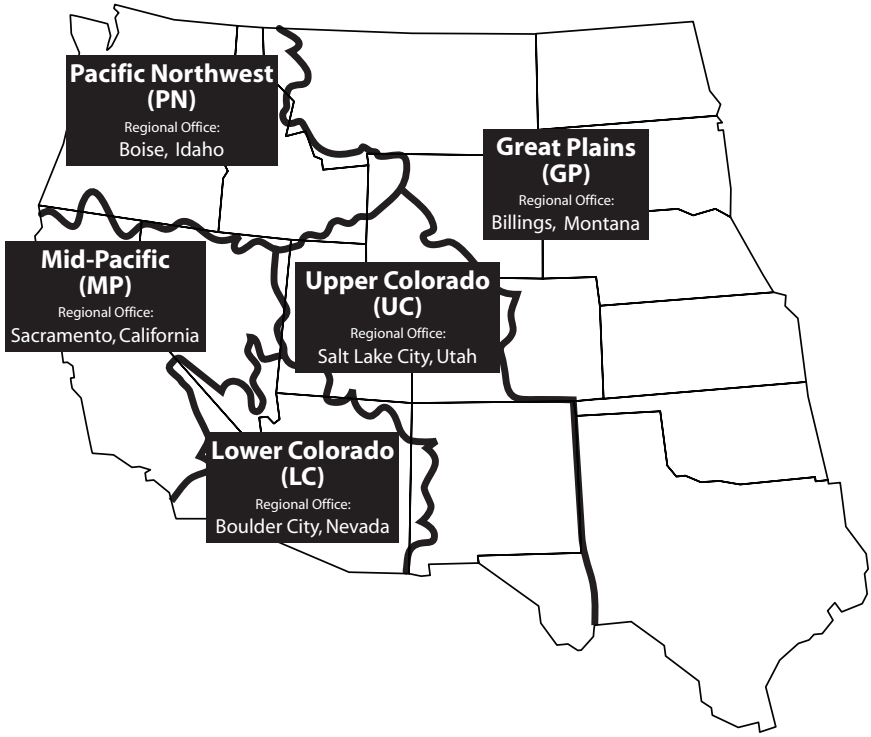


FIGURE 2.2 Reclamation's regions and regional offices.

have been transferred to water and power authorities and other local beneficiary organizations.[3]

The SSLE Office, established in 2001, is in Denver. In addition to security, law enforcement, and program and emergency management, the SSLE is also responsible for the safety of dams program and the safety office. The committee was not asked to assess the safety of dams or the safety programs. The SSLE also has a three-person liaison office in Washington, D.C., that serves as liaison with DOI and with Congress, OMB, and other organizations (Figure 2.3).

BOR was first granted law enforcement authority in November 2001. P. L. 107-69 gave Reclamation law enforcement authority for misdemeanor-

[3]The Reclamation Extension Act of 1914 required the payment of operating and maintenance costs; recognized legally organized water users' associations and irrigation districts; and authorized the transfer of project facilities operations and maintenance to water districts (BOR, 1972).

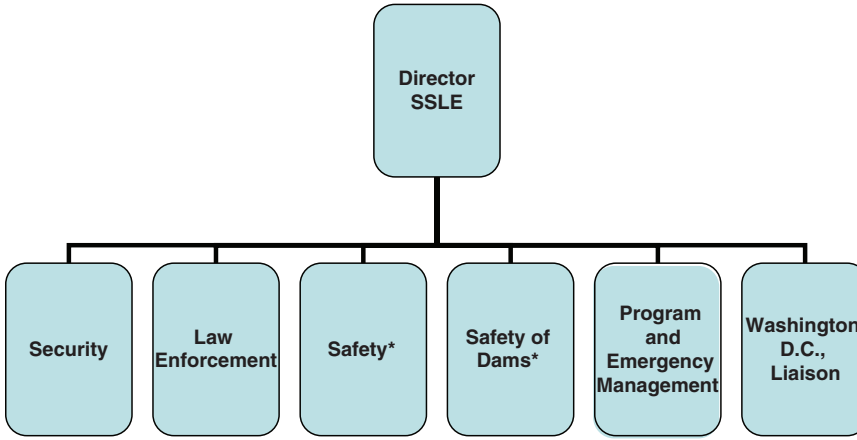


FIGURE 2.3 Organization of SSLE Office. *Not reviewed in this study.

level crimes such as theft or vandalism on or to its property and facilities. The legislation allows Reclamation to use law enforcement personnel from DOI or other federal agencies except the Department of Defense. It does not address issues of security or antiterrorism, nor does it allow Reclamation to directly hire law enforcement personnel.

SSLE has a staff of approximately 48 full-time equivalent positions. Its annual site security budget[4] has fluctuated, from about $54 million in FY 2003 to around $40 million currently. It contracts with private-sector firms for site security and for some tasks related to intelligence gathering and analysis and emergency support. SSLE works with OLESEM, the CIO, and BOR's Technical Services Center (TSC) to plan and implement some aspects of the program. SSLE also works with water districts, local law enforcement, BOR stakeholders, and outside organizations, including the DHS, FEMA, the Federal Protective Service (FPS), and the Federal Bureau of Investigation (FBI).

SECURITY

SSLE's security group provides technical expertise and is responsible for security assessments and risk management coordination, facility security and design improvements (e.g., closed-circuit TV cameras, fences, access control systems), personnel security (background checks), opera-

[4]SSLE also has a Safety of Dams and Emergency Management budget.

tions security, and interagency coordination. The security group is headed by the chief security officer. Twelve additional staff positions are located in the Denver office, and one regional security officer (RSO) is assigned to and works from each of the five regional offices. The RSOs serve as a technical link between the Denver office and the regional and area offices. They are responsible for regional implementation of security directives, standards for identifying and safeguarding sensitive documents, and background investigations of personnel, among other duties. Additional support for risk assessments and for design and engineering studies is provided by the TSC.

Security Assessments and Risk Management Coordination

With relatively limited resources and more than 450 dams that vary greatly in size, siting, amount of power and water delivered, distance from downstream population centers and size of those populations, relationship to local and regional economies, and the magnitude of the consequences of their failure, it is not possible (and may not even be desirable) for Reclamation to provide the same level of protection for all of its facilities. BOR has recognized the need for an approach that pays more attention to those dams and facilities that are more attractive targets and where the consequences of a successful attack would be the greatest and invests more resources in their protection.

Although risk can be measured in a variety of ways, it is most commonly assessed as a function of the probability of an event and the consequences of the event. A risk management program for a large inventory of facilities entails a screening process to identify those facilities in the inventory that require closer scrutiny, risk assessments to identify vulnerabilities of individual facilities and potential consequences of a failure, a process for quantifying and evaluating the costs and benefits of technologies and other risk mitigation measures, and decision analysis. The overall goal of a risk management program is to establish a transparent and rational decision-making process that optimizes security across the entire facilities inventory.

A risk management program for dams and other facilities should incorporate a screening process that uses a common basis for evaluating an inventory of facilities according to their security-related risk profiles. A screening process might begin with a review of security-related dam attributes such as “criticality” (how important the dam is to the organization’s mission) and “vulnerability” (the likelihood that an attack will

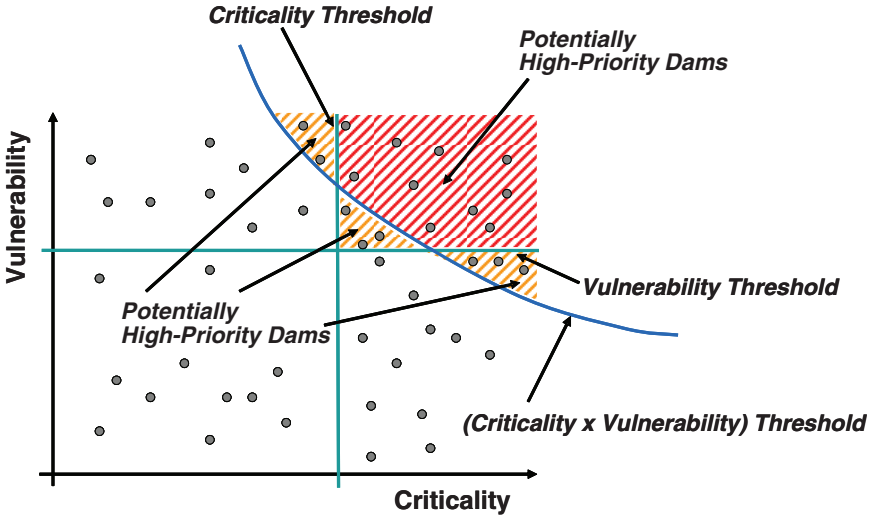


FIGURE 2.4 Notional results of screening by criticality and vulnerability to identify dams that need to be given high priority.

be successful).[5] By assigning numerical values to these attributes (say, on a scale of 1 to 5), criticality and vulnerability scores can be calculated for each dam. Aggregate scores of many dams can then be plotted on a graph. This will facilitate identification and prioritization of dams with relatively high risk—that is, those with high criticality and high vulnerability (Figure 2.4).

A variety of ways to assess risk have been developed. Generally they are analytic, quantitative, and probabilistic. They should also be consistent with accepted practices and transparent. Risk assessment typically starts by developing threat or security scenarios (e.g., use of a truck bomb) and then goes on to look at the potential consequences of a successful attack, to analyze vulnerability (e.g., measures in place to deny, deter, delay, respond to, or defeat the attackers), and to assess the threat (the likelihood or probability of attack from an adversary's perspective). These elements are systematically considered to determine which assets

[5]Criticality might include population within inundation zones, the iconic status of the dam, economic consequences of interrupting power and water supplies, and the time required to bring a damaged facility back on line. Vulnerability might include construction type, operational features, accessibility, security and emergency response capabilities, and previous threats.

warrant the most protection, how this protection can be provided in a cost-effective manner, and how damage can be minimized in the event of a successful attack.

Immediately after the 9/11 attacks, BOR staff with expertise in security, engineering, and dam operations and maintenance developed a process for screening Reclamation's inventory of dams to identify those whose failure as the result of an act of terrorism would have the severest downstream consequences and the most critical impacts from loss of mission, such as providing water and power. A 10-tiered categorization process was used to assign priority for security risk assessments. Five facilities were designated national critical infrastructure (NCI) facilities. In early 2002, BOR contracted with the Defense Threat Reduction Agency (DTRA) to assess vulnerabilities at its NCI dams using the Balanced Survivability Assessment method. This method focuses on identifying vulnerabilities at a dam site that could be exploited by a well-trained team of terrorists and then identifying mitigation measures for those vulnerabilities. It does not include a threat assessment or an assessment of potential consequences.

In the same time period, four private contractors and one semipublic agency were hired to perform Risk Assessment Methodology–Dams (RAM–D) assessments for the next 50 facilities on the priority list. RAM–D is a qualitative assessment of probability of attack, consequences, and security system effectiveness developed by an interagency committee in consultation with the Department of Energy's Sandia National Laboratories. In late 2002 and early 2003, all of the recommendations for improvements resulting from the 55 assessments were reviewed and evaluated by a security advisory team (SAT) comprising staff from SSLE and BOR's regional and area offices and outside experts from the U.S. Army Corps of Engineers (USACE) and Sandia National Laboratories. The SAT evaluated the recommendations based on the extent to which they could potentially reduce risk and the feasibility of implementing them. Decision documents were then prepared for each of the 55 facilities evaluated and presented to the SSLE director, to the relevant regional directors and area office managers, and to the deputy commissioner and the commissioner for their approval, with the concurrence of DOI's assistant secretary for water and science. The procedure is intended to ensure that recommendations have been critically evaluated, are cost effective, and reduce risk and that risk management strategies are consistently applied across Reclamation (OMB, 2007).

From mid-2003 to early 2006, the next 225 facilities were evaluated by Reclamation staff using the Matrix Security Risk Assessment (MSRA) methodology, which is a qualitative evaluation of threats, vulnerabilities, and consequences. The SAT reviewed and evaluated the assessments,

prepared decision documents, and sent them forward for concurrence by the SSLE director and the respective regional directors and area office managers.

As of June 2004, the 10 tiers of facilities had been recombined into 5 categories: NCI, major mission critical (MMC), mission critical (MC), project essential (PE), and low risk. MMC facilities are defined as facilities that are characterized by large, multipurpose features and high downstream hazards and that are so vital to the nation that their incapacitation or destruction would have a debilitating effect on national security, regional economic security, and/or regional public health or safety. MC facilities are defined much like MMC facilities except that they are moderately large and their downstream impacts would be more moderate. PE facilities are Reclamation facilities that are essential to a particular project and the locale and whose incapacitation or destruction would have a significant impact on local economic security, public health, or safety, or any combination thereof. Low-risk facilities, which might include small office buildings and project support facilities, are defined as those whose loss would not be a substantial loss to the public or BOR.

Over time, as more information on the vulnerability of specific types of dams becomes available through research and testing, some dams have been recategorized.

The SSLE plans to conduct comprehensive security reviews (CSRs) for all 178 critical facilities every 6 years. Periodic security reviews (PSRs) are to be conducted by the regional offices 3 years after a CSR is conducted.

In a few cases, risk assessments at BOR dams have been conducted by outside agencies, including the California Department of Homeland Security and the California National Guard. However, these assessments were not always made available to Reclamation or the appropriate area offices.

Facility Security and Design Improvement Projects

One outcome of the risk management process is the identification and prioritization of facility security and design improvement projects intended to mitigate vulnerabilities. Such projects involve access control systems; perimeter, vehicle, and boat barriers; closed circuit TV monitoring systems; intrusion detection and alarm systems; lighting; security control centers; and guard/response personnel. Some projects resulted in closing roads traversing dams or limiting access to them and rerouting traffic to existing or new roads. At least two new bridges are being built in conjunction with highway realignments to move traffic off critical dams.

Reclamation has identified specific upgrades required at individual facilities and prioritized them according to the criticality of the facility, project feasibility, and the degree to which the project will mitigate risk. As funding becomes available, the projects are designed and implemented by the security group with support from the TSC.

During the site visits, committee members were told that some water and power authorities that operate BOR facilities had paid directly for security upgrades, including security guards. In one case the water and power authority collaborated with BOR staff to identify security improvements and then installed the improvements at its own expense. However, security upgrades by water and power authorities are not necessarily coordinated with the SSLE or the field offices. Nor do all water and power authorities have the resources to implement such upgrades.

Personnel Security

Homeland Security Presidential Directive 12 (HSPD-12), issued in August 2004, requires that a policy be developed for standardizing the identification procedure for federal employees and contractors. This requirement is intended to eliminate the wide variation in quality and security of forms of identification for gaining access to secure federal facilities. Federal agencies must develop and deploy for their contract personnel and employees a personal identity verification (PIV) credential that is secure, reliable, and interoperable at all federal agencies.

At BOR, the PIV process is used for conducting background checks on all BOR employees and the hundreds of contract workers who are active in new construction, operations, and maintenance projects at the various facilities. To comply with the PIV requirement, the security group has one staff position in Denver and the regional security officers to process and adjudicate background investigations and reinvestigations, issue and verify national security clearances, and maintain personnel files and databases. During one of the site visits, BOR staff reported that it can take as long as 6-8 months to complete the PIV process for one individual.

Given this time lag, the field offices have had to make accommodations for contractors so they can complete their jobs. For example, at one of the NCI sites, an escort is provided for workers for up to 180 days or until the project or the PIV process has been completed. At another NCI site, it was estimated that contractors may lose an hour or so of productivity per day per worker owing to the time it takes for identity verification and search procedures when entering or exiting some of the zones at the site. Such costs are probably passed along to BOR in the form of higher bids for projects.

LAW ENFORCEMENT

SSLE's Law Enforcement Office is responsible for the following:

- Enforcing federal laws and regulations;
- Conducting investigations;
- Gathering, analyzing, and disseminating intelligence;
- Conducting threat assessments;
- Conducting law enforcement training; and
- Conducting security and law enforcement exercises.

Within Reclamation, law enforcement's primary goal is to

> assure the security for Reclamation resources and facilities, and the safety of employees and the visiting public. Working strategically and in close partnership with security personnel, assigned law enforcement personnel identify and investigate potential threats and implement effective security and response procedures. Coordination with other law enforcement, security, and intelligence agencies and organizations is crucial. (BOR, 2005, p. 12)

The law enforcement administrator (LEA) is responsible for promulgating policy, procedures, and standards for Reclamation's law enforcement authority. The LEA oversees a staff of 12, including 6 regional special agents (RSAs). One RSA is assigned to each region and one to the Grand Coulee Dam. The RSAs are assigned to BOR through an interagency agreement with DOI's Bureau of Land Management (BLM). BLM provides administrative oversight for the agents, while SSLE oversees their day-to-day operations. Additional support for intelligence gathering and dissemination is provided by private-sector contractors (Figure 2.5).

The RSAs have multiple responsibilities. They serve as the primary law enforcement resource for the regional directors, area office managers, and field personnel. They gather and analyze security-related information for Reclamation's facilities, projects, and properties, and they conduct threat assessments as part of the risk management process. RSAs serve as liaisons to federal, state, tribal, and local law enforcement and oversee contracts and cooperative agreements for law enforcement assistance.

Law enforcement officers are authorized to carry firearms within the perimeter of a BOR project or on BOR lands and to make arrests, execute warrants, and conduct investigations. Investigations may pertain to violations of federal law, serious misconduct (or allegations thereof) by Reclamation staff, or administrative issues. However, an RSA or other Reclamation officer can conduct an investigation only if the federal law enforcement agency (typically the U.S. Marshals Service or the FBI)

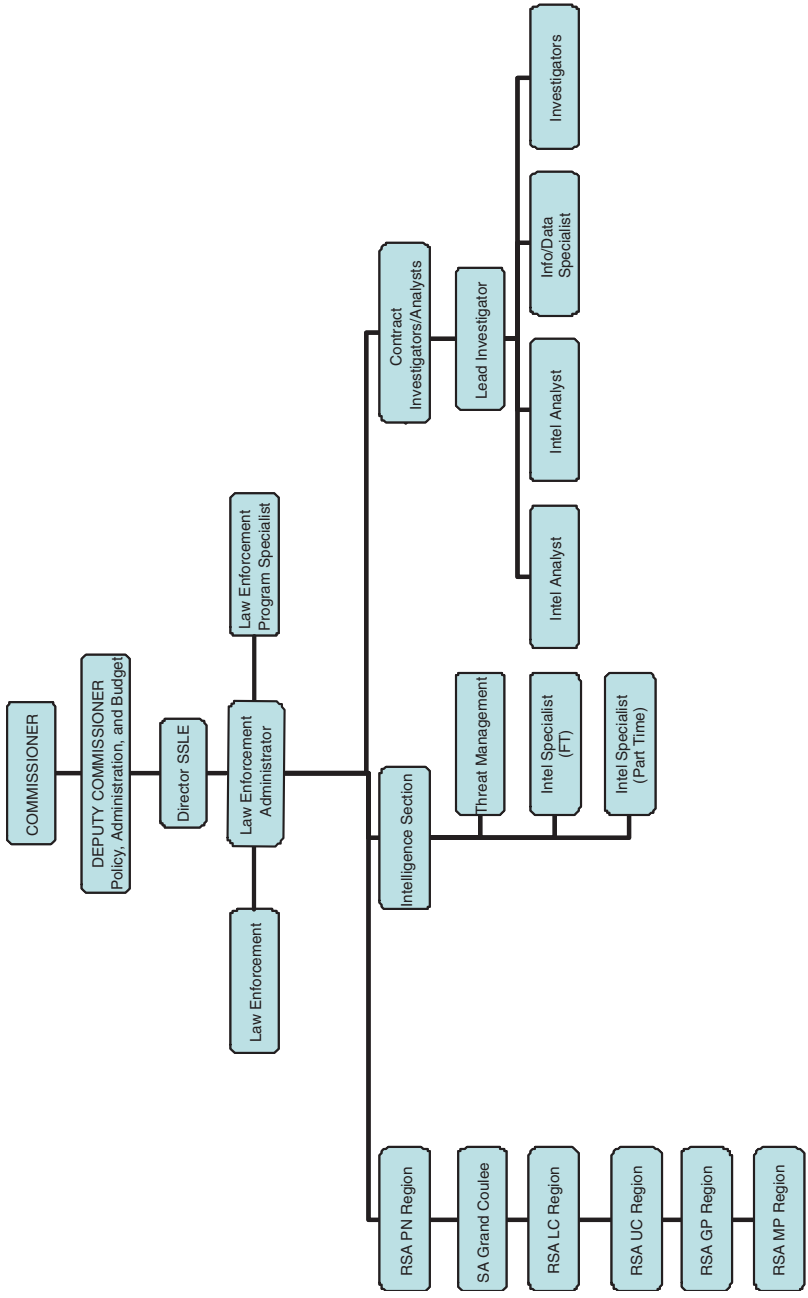


FIGURE 2.5 Organization of SSLE's law enforcement group. SA, Special Agent.

having investigative jurisdiction decides not to investigate an alleged offense.

Some Reclamation facilities have contracts with private-sector firms to provide site security guards. The primary responsibility of site security guards is to protect people and property by controlling access to facilities and by deterring individuals who might consider attacking them. They are not law enforcement officers and must call on federal or local law enforcement personnel when a criminal act is suspected. Some site security guards are authorized to carry guns, but others are not.

In the law enforcement profession, the police play four roles in their organization and the community: crime fighting, partnership, prevention, and problem-oriented policing or problem solving. Crime fighting involves answering calls, investigating crimes, and making arrests. Partnership involves interaction with peers and colleagues, external police agencies, and the community. To establish partnerships, police must first develop the respect, trust, and support of the people and organizations they work with. They build on this foundation through active engagement with their peers, external agencies, and the community. If trust and support are nonexistent, then partnerships fail. Prevention involves proactive police work—anticipating problems of disorder and then deterring them. Problem-oriented policing or problem solving includes a thought process whereby police identify specific problems, analyze their component parts, provide adequate responses to those problems, and then assess how well they did in solving them. This process is intended to identify the root causes of crimes and intervene before they get out of control. It can also be used to prioritize the types of crimes and problems that may exist within an area or jurisdiction and develop strategies to address them.

At Reclamation, the crime-fighting role has been contracted out to local law enforcement with minimal oversight by the RSAs. Because their jurisdictions are so vast, the RSAs do not have the time or the resources to deal with crime. For the most part they receive information from BOR personnel or local law enforcement about incidents at or near dams in their region and they relay that information to the LEA in Denver.

Partnerships have been formed throughout the regions with local law enforcement, National Park Service rangers and Fish and Wildlife rangers, contractors, and private security firms, among others. Some of the partnerships are based on informal relationships, while others are made through memoranda of understanding (MOUs). Partnerships to share intelligence-related information have also been established through the FBI's Joint Terrorism Task Forces (JTTFs), discussed later in this chapter.

The task of prevention is primarily carried out by the RSAs at the NCIs through facility security measures, education, and training. Problem-oriented policing or problem solving has been used sparingly by Reclama-

tion. The committee did not see much evidence of problem identification or analysis, targeted responses, or evaluations of their work. Reclamation is working to improve the reporting of crime and security-related incidents and to implement DOI's Incident Management and Reporting System.

Security Incident Response

In the event of a security breach or actual attack on a BOR facility, appropriately trained and equipped security and/or law enforcement personnel must respond. With a few exceptions, that response will come first from local law enforcement entities. DOI policy is that response activities should be managed at the lowest possible organizational level. According to the National Incident Management System (NIMS), the secretary of Homeland Security will coordinate a field response to a terrorist attack or other emergency only if (1) a federal department or agency acting under its own authority has asked the secretary for assistance; (2) the resources of state and local authorities are overwhelmed and federal assistance has been requested by the appropriate state and local authorities; (3) more than one federal department or agency has become substantially involved in responding to the incident; or (4) the secretary has been directed by the President to assume responsibility for managing the domestic incident (EOP, 2003a, p.1).

Facility and area office staff, which may include on-site law enforcement or site security guards, are responsible for identifying suspicious activity or an actual breach of security at a facility, for notifying the regional office and other appropriate responders (i.e., local law enforcement), and for securing the premises until backup arrives, typically in the form of local law enforcement.

If a facility was damaged such that people downstream were threatened, BOR personnel would notify the appropriate local authorities, who would notify their constituencies and begin evacuation. In an actual incident, the area office manager would probably, at least for a time, be the public face of Reclamation, answering questions from the media and others.

Hoover Dam is Reclamation's only facility with an on-site, in-house police department, which includes a tactical team that could theoretically respond quickly to an evolving situation. At Grand Coulee Dam, the tactical response capabilities lie with members of the security force that guards the facility. At Folsom Dam, any initial tactical response would come from the Sacramento County sheriff's department, the parent agency of the contract deputies who provide on-site security for the installation. At Shasta and Glen Canyon dams, the initial response would come from local county sheriff's offices.

Less robust response capabilities are available at other BOR facilities. Dams on the lower Colorado River south of Hoover Dam, for example, employ small armed cadres of private security guards. In other cases, the responding force might be rangers from the National Park Service or the U.S. Fish and Wildlife Service.

For Reclamation, then, the interface between the initial responders and the law enforcement entities who follow up will be substantially different at each facility. Thus, Reclamation area office and regional personnel, police from other federal agencies, and the local law enforcement personnel who are expected to respond to a terrorist or other malicious act must make appropriate arrangements for working together in a security-related incident.

First responders, including local law enforcement, typically use a standardized incident management system called the Incident Command System (ICS) to manage resources and provide unity of command during a crisis. Incident action plans are used to communicate the objectives of operational and support activities.

Security and Law Enforcement Exercises

Security and law enforcement exercises are conducted to allow an organization's decision makers, personnel, and partners who would respond to a security-related incident to identify limitations and problems in existing response plans and correct them in advance of an event. Exercises bring together people who might not otherwise be acquainted and help them develop working relationships. They can be used to improve response plans, improve the quality and capacity of the response, and build relationships. The last-mentioned is especially important because in a crisis it will be the personal and working relationships among the responders that will determine the success or failure of the response, not the written plan.

FEMA's National Preparedness Directorate has established a Homeland Security Exercise and Evaluation Program (HSEEP) that constitutes a national standard for all such exercises. HSEEP is a capability- and performance-based program that provides a standard methodology and terminology for the design, development, conduct, evaluation, and improvement of training exercises (HSEEP, 2007).

Exercises can take several forms—tabletop, functional, full scale—that vary in purpose, format, and resources required. Tabletop exercises are intended to stimulate discussion of the various issues surrounding a hypothetical situation. They simulate a security-related emergency situation in a stress-free, informal environment. The focus is on training, decision making, coordination, and communication roles, procedures,

and responsibilities. The exercise itself may be aimed at facilitating an understanding of concepts, identifying strengths or shortfalls, and/or achieving a change in attitude (HSEEP, 2007). A security-related scenario is developed. Staff from all levels of an organization such as Reclamation, representatives of its partners, and staff from other federal, state, and local responders gather around a table to discuss what might happen in the context of the scenario. They discuss any problems that arise and identify changes needed for a more effective response. Tabletop exercises require a modest commitment of funds and personnel time and expertise and can be effective in improving response plans and procedures. However because they lack realism and the pressures of real-time decision making and action, they are not a true test of response capability (HSEEP, 2007)

The objective of a functional exercise is to test and evaluate the effectiveness of one or more specific functions in real time. A functional exercise is characterized by the simulated deployment of resources and personnel, rapid problem solving, and a highly stressful environment (HSEEP, 2007). The focus of a functional exercise could be public notification and warning systems, decision-making processes, communication and coordination procedures, or the allocation of resources and personnel. Such exercises are carefully scripted, planned, and sequenced to simulate a real-life situation. During the exercise, personnel involved in policy, coordination, and operations for the chosen function practice their response in a realistic way. Problems and issues that come up during the response are identified, and methods for resolving them are suggested. Functional exercises require a greater investment of resources and time than tabletop exercises, but they also provide a more realistic test of response capabilities.

One variation on a functional exercise that can provide valuable information about preparedness is "red teaming." FEMA defines a red team as a group of subject-matter experts with various disciplinary backgrounds that provides, in effect, an independent peer review of plans and processes. A red team acts as the adversary's advocate, and participants knowledgeably role-play the adversary in a controlled, realistic, interactive manner during operations planning, training, and exercising (HSEEP, 2007, p. B-26). Red teams can be used in prevention-focused functional exercises that concentrate on exercising the plans, policies, procedures, agreements, networks, and staffs of law enforcement agencies with counterterrorism missions, such as SSLE's LEA.

A full-scale exercise is designed to challenge the entire response system in a highly realistic and stressful environment. It is a multiagency, multijurisdictional activity involving the actual deployment of resources in a coordinated response as if a real incident had occurred (HSEEP, 2007). Typically the exercise would take place at a facility and would employ simulated attacks and victims. To the extent possible, the actual equipment

and personnel who would be involved in a response participate in the field exercise. All decisions and actions by the participants occur in real time and generate real responses and consequences for other players. In this way, all functions and relationships required for a response can be tested and evaluated. Typically, a formal after-action report identifying problems and recommending solutions is produced and disseminated to the appropriate parties, including managers, throughout the organization.

Full-scale exercises require a significant investment of time and resources if they are to be useful. It may, for example, take a year or longer to develop a detailed exercise package with a carefully thought-out set of objectives, a well-planned and simulated scenario, a logistics plan, and the elements to be covered in the after-action report. The exercise itself will require significant amounts of staff time. Funding will be needed for planning and follow-up and for travel expenses to bring off-site personnel to the site of the exercise.

Reclamation has conducted tabletop and functional exercises at some of its critical facilities. Full-scale exercises have been conducted at Grand Coulee, Flaming Gorge, and Hoover dams. The SSLE plans to hold additional exercises as time and funds permit. Exercises have also been conducted by local governments. In these cases, Reclamation's area offices did not always receive a summary of the results or the final report. To the committee's knowledge, SSLE's LEA has not held any red-teaming, prevention-focused functional exercises.

Intelligence Gathering, Analysis, and Dissemination

Federal initiatives to consolidate and centralize control over numerous components of the national intelligence apparatus speak clearly of the critical importance of intelligence to security. Reclamation recognized this and created an intelligence element within the law enforcement component of SSLE (see Figure 2.5). Intelligence procedures include maintaining a database of intelligence, incidents,[6] and international visitors (OMB, 2007). The LEA compiles and analyzes numbers, types, and patterns of incident reports to assist law enforcement and security officers in the protection of Reclamation's facilities and people. It provides classified intelligence briefings to senior management as well as intelligence and officer safety information to area and field offices, as appropriate.

The Denver headquarters intelligence group receives intelligence-related information from the Interagency Forum on Infrastructure Pro-

[6]Intelligence incidents include bomb threats, burglaries/thefts, criminal activities, cyber-attacks, overflights of facilities, suspected surveillance, suspicious activities, trespassing, vandalism, and weapons.

tection, DOI's Watch Office, the FBI, and state agencies, including the Arizona Counter Terrorism Information Center, the Colorado Information Analysis Center, and the Nevada Emergency Operations and Notification Network. Other sources of information include daily or weekly bulletins and alerts, publications, television, and the Internet. The intelligence group also works with Reclamation's international affairs office to ensure that appropriate background checks are conducted for international groups who visit Reclamation facilities and that facility personnel are notified of such visits and given a list of cleared individuals (OMB, 2007).

The RSAs receive security-related information from the Denver office and through the FBI's JTTFs, which operate in every part of the country where there is an FBI office. In the Great Plains region, for example, 12 to 14 JTTFs are operating. The RSAs attend JTTF meetings as time and resources permit, and the JTTFs inform the RSAs of any security-related developments. The RSAs also receive information from the LEA, on-site BOR personnel, local law enforcement agencies, the county sheriff, other partners, and the local community. The RSA may communicate such information to the LEA and the FBI.

Developing intelligence through collaborations and liaisons requires good internal and external working relationships, partnerships, and an effective communications system. For example, at one site, the managers of a nearby boat rental business observed some customers behaving suspiciously. The business managers reported this behavior to the local National Park Service ranger, who in turn reported it to the RSA. At another site, when a suspicious package was found on a dam, the RSA was not able to contact the appropriate FBI office directly and had to leave a voice-mail message on the phone. The RSA alerted the county sheriff, who blocked access to the site from the road and the reservoir.

In some cases, if the RSA receives intelligence deemed "sensitive" from the FBI or others, he or she may be restricted in passing that information along to others, including a facility's operators, managers, or even the RSO. Such restrictions may be counterproductive to the extent that the field staff in the best position to prevent or deter a security-related incident are not given the information that would help them to do so.

INCIDENT RESPONSE MANAGEMENT

Reclamation's emergency management program was established in conjunction with the safety of dams program. The emergency management program is intended to provide for the safety of the public and to protect environmental resources from incidents at its facilities by (1) taking reasonable and prudent actions necessary to ensure timely notification of such incidents to potentially affected jurisdictions so that the public can

be warned and evacuated and (2) defining what the program needs to allow its line managers to be self-regulatory, to be responsive to public safety, and to satisfy legal requirements during operations or emergency incidents at its facilities.

It is not within Reclamation's legislative authority or responsibility to warn directly or to evacuate the public in the event of a safety-related dam failure or the threat of a failure. The underlying premise is that if a dam is in danger of failing due to torrential rains, a design flaw, or other safety-related event, there will be sufficient time to notify local authorities and to evacuate people before downstream flooding occurs. This procedure does not take into account a dam failure caused by a malicious act in which there may be little or no advance warning of downstream flooding.

SSLE's Program and Emergency Management Office (PEMO) is responsible for centralized fund management for site security, emergency management, IT project management for SSLE, congressional and audit liaison, policy, and special projects. The office has eight staff members, including the program chief. Additional support for emergency management is provided by a private-sector contractor and the TSC.

Reclamation's emergency management functions are conducted in accord with DOI policy,[7] which covers the Continuity of Operations Plan (COOP), the National Security Emergency Preparedness (NSEP), the coordination of emergency incidents, and the National Response Plan (NRP) coordination. PEMO is responsible for Reclamation's compliance with these policies. It coordinates its activities through the designated emergency manager and COOP manager in each region.

Individual area offices develop COOP plans so that Reclamation can continue to carry out its essential functions during an emergency. SSLE provides training and technical support and oversees regional COOP activities. An emergency operations center (EOC) is maintained in Denver to provide coordination and enhance communications during periods of high threat or actual emergency situations. Reclamation also supports the DOI COOP by providing an alternative operating site in Denver.

Reclamation has developed emergency action plans (EAPs) for many years as part of its safety of dams program. The plans are updated annually and exercised every 3 years. PEMO coordinates a variety of emergency communication capabilities, both unclassified and classified. It also provides 24-hour duty officers, an Emergency Notification System

[7]Department of the Interior, *Departmental Manual,* Part 900, Emergency Management Program, Chapters 1-5. Available at http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3693. Last accessed November 14, 2007.

for Reclamation employees, and an interface to the DOI's Watch Office in Washington, D.C.[8]

Under the National Response Plan, Reclamation is the executive agent for the DOI for Emergency Support Function for Public Works and Engineering and supports the Natural and Cultural Resources and Historic Preservation function. In 2005, BOR supported the response and recovery efforts for Hurricanes Katrina, Rita, and Wilma.

INFORMATION AND INFORMATION TECHNOLOGY SECURITY

Reclamation's Information Technology (IT) Security and Management Program was formally established in 2000, one year before the SSLE. Responsibility for information and IT security resides with the Office of the Chief Information Officer (CIO). The program is guided by five objectives:

- Ensure the safety of personnel and the public;
- Protect the federal investment;
- Take all reasonable precautions to prevent IT vulnerabilities from adversely affecting the mission;
- Ensure the integrity of IT services to authorized project beneficiaries by determining acceptable risk levels and conducting periodic IT system audits to ensure compliance; and
- Provide for timely delivery of services via IT.

Reclamation's IT Division treats SCADA systems security much like computer security using IT legislation, regulations, and other guidance to establish the baseline. SCADA systems primarily involve (1) water and water treatment control systems to monitor levels, flows, salinity, turbidity, dissolved gases, and the like and (2) electric power generation control systems to monitor the condition of generators, transformers, motors, switches, breakers, and hydraulic and hydromechanical cooling systems. A number of physical and personnel security measures have been implemented to protect these systems from cyberattacks.

The IT Division establishes background check requirements for key personnel and coordinates access to its systems with the BOR's human resources office, the SSLE, and facility operations. Security is independently tested and operation is authorized by management officials based

[8]The Watch Office is administered by OLESEM. It is responsible for coordination of law enforcement, emergency management, and security requirements placed on DOI after 9/11, among other things. It operates 24 hours per day, 7 days per week.

on acceptable levels of risk. Information security criteria developed by the National Institute for Standards and Technology provide the baseline.

SCADA systems associated with power plants are not always under the control of BOR. For example, some power companies control electricity generation while BOR controls the water flow. Good working relationships among the various operators are critical for coordination on a routine basis and during a security-related incident.

RESOURCES AND FUNDING

Before the 9/11 attacks, Reclamation's budget for security-related activities was about $1.35 million per year. After that, Congress gave Reclamation supplemental funding to make immediate security-related upgrades to its facilities.[9] However, Reclamation has primarily funded the security program by redirecting resources from other programs, including dam safety and facilities maintenance (Table 2.1). This approach to funding security has created internal tensions and resentment and may hurt the other programs over the long term.

By law,[10] the costs incurred by Reclamation to construct, operate, and maintain project facilities for the purpose of providing benefits to project beneficiaries (such as irrigation, municipal, and industrial water users and consumers of power generated at BOR facilities) may be either nonreimbursable or reimbursable by those beneficiaries. Nonreimbursable costs are fully paid by the government. Reimbursable costs are recovered in full or in part from project beneficiaries in the form of annual repayments, sales of water and power, or advanced funding. For example, under the safety of dams program, the costs of some safety-related items are split between BOR (85 percent) and beneficiaries (15 percent).

To supplement security-related funding and reduce pressures on other programs, Reclamation has sought to make some security-related activities, especially site security guards, fully reimbursable, thereby shifting the funding responsibility to water and power authorities and other beneficiaries. Reclamation currently devotes approximately $20-$21 million of its $50 million budget to paying for security guards.

In its FY 2005 Conference Report, Congress instructed Reclamation not to seek reimbursement and to submit a report explaining the planned

[9]$30,259,000 in FY 2002 and $25 million in FY 2003.

[10]The Reclamation Project Act of 1939 provided authority for project costs to be allocated between reimbursable and nonreimbursable purposes, authorized a ceiling on charges to irrigators based on an ability-to-pay concept, and provided authority for the secretary to defer repayment obligations under certain circumstances. The act also provided for reimbursable project costs associated with irrigation or municipal and industrial purposes to be recovered through repayment or water service contracts (NRC, 2006).

TABLE 2.1 Reclamation's Security Program Funding (thousands of dollars)

	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007 Requested
Site security enacted budget	1,043	1,755	28,440	28,583	43,216	40,000	39,600
Site security supplemental		30,259	25,000				
Site security subtotal	1,043	32,014	53,440	28,583	43,216	40,000	39,600
Emergency management subtotal	309	330	334	450	451	1,360	1,346
Total	1,352	32,344	53,774	29,033	43,667	41,360	40,460

expenditures. In FY 2006 Reclamation again proposed reimbursement of some costs. The FY 2006 Conference Report instructed Reclamation to collect $10 million in reimbursement instead of the $16.3 million that would otherwise have been reimbursed and requested another report. In FY 2007 Reclamation's budget request includes full reimbursement for guard and patrol costs. The issue remains under discussion in 2008.

REFERENCES

Bureau of Reclamation (BOR). 1972. *Federal Reclamation and Related Laws Annotated, Volumes I-III.* Washington, D.C.: Bureau of Reclamation.

BOR. 2005. *Security Program.* Washington, D.C.: Bureau of Reclamation.

Homeland Security Exercise and Evaluation Program (HSEEP). 2007. *Volume 1: HSEEP Overview and Exercise Program Management.* Available at https//:hseep.dhs.gov/support/VolumeI.pdf.

National Research Council (NRC). 2006. *Managing Construction and Infrastructure in the 21st Century Bureau of Reclamation.* Washington, D.C.: The National Academies Press.

Office of Management and Budget (OMB). 2007. *Program Assessment. Bureau of Reclamation—Site Security.* Available at www.whitehouse.gov/omb/expectmore/summary/10003701.2005.html.

3

Assessment of Reclamation's Security-Related Processes

The committee was tasked to assess Reclamation's security, law enforcement, and incident response processes and functions in order to determine whether it is appropriately structured and has the expertise required to protect its infrastructure and its people. A related task was assessing working relationships with other organizations having security and law enforcement functions, including other units in the Department of the Interior (DOI) and other federal, state, and local agencies.

To address this task, the committee relied on briefings from and discussions with personnel from the Security, Safety, and Law Enforcement (SSLE) Office, regional and area offices, regional special agents (RSAs), regional security officers (RSOs), facility operators, contractors, local law enforcement officers, site security guards, and water and power authority staff. The discussions took place in Denver and at various Reclamation sites. The committee also reviewed some classified and for official use only (FOUO) documents. The committee members' experience and expertise in security, law enforcement, risk assessment, and engineering were important to the formulation of their findings.

Chapter 3 first presents the committee's observations and findings about Reclamation's processes and functions for security assessments and risk management, personnel security, facility security, incident response, exercises and training, and intelligence gathering and dissemination. Observations and findings on working relationships follow. Chapter 3 concludes with a discussion of staff expertise.

SECURITY ASSESSMENTS AND RISK MANAGEMENT

Reclamation has developed a risk management program that incorporates a screening procedure; development of threat scenarios; vulnerability and risk assessments for individual facilities; a cost-benefit analysis for risk mitigation measures; and a decision analysis framework.

The grouping of Reclamation's facilities into categories that reflect relative risk and consequences (screening procedure) has been useful in assigning priority for mitigation projects and resource allocation. Several different methods, including Risk Assessment Methodology–Dams (RAM–D), Matrix Security Risk Assessment (MSRA), and a balanced survivability assessment approach, have been used to conduct threat and vulnerability assessments; these methods are all accepted standards and are appropriate. Nonetheless, the committee identified areas where Reclamation could refine elements of its overall risk management program now or in the future, as described below.

Risk Assessment Methods

Since the 9/11 attacks, the field of risk and threat assessment has been evolving rapidly. New methods are being developed that focus on intentional malicious acts of destruction committed by human beings as opposed to risks posed by natural hazards. Recently, the Department of Homeland Security (DHS) reviewed more than 100 risk assessment methods to try to identify those that could potentially be applied consistently across infrastructure sectors (e.g., transportation, dams, water supply). Among those considered were the Strategic Homeland Infrastructure Assessment, Risk Analysis and Management for Critical Infrastructure Protection, Critical Asset and Portfolio Risk Analysis (CAPRA, described in Appendix C), Maritime Security Risk Analysis Method, and the Critical Infrastructure Common Risk Model. It is not yet clear whether a cross-sectoral approach can be effective or whether a generalized methodology will have to be customized for dams or supplemented by an alternative. Reclamation security managers should stay abreast of these developments and be ready to use risk assessment methodologies recommended by the DHS and methodologies that are customized to the specific requirements of dam security, such as RAM–D.

New methods for analyzing the costs and benefits of mitigation measures and prioritizing projects are also evolving. One such method is OVI (occurrence, vulnerability, importance), which is a framework for prioritization that ranks potential security projects and allows them to be compared to other projects under consideration. The framework was developed through the National Research Council's (NRC's) Transportation Research Board and is being used by the Federal Highway Admin-

istration and the New York City Department of Transportation to make decisions about retrofit projects. The OVI method has built-in mechanisms and quantifying actions that allow for relative, not absolute, rankings of projects. An example of how this method might be used for dams is included in Appendix C.

Finding: The risk management process that Reclamation has developed to assign priority for conducting threat and vulnerability assessments, security improvements, and resource allocation is appropriate. Elements of this process, however, need to be continually improved and refined as threats emerge, risk assessment methods evolve, and research-based information becomes available.

Categorization of Facilities

Since initially assigning its facilities to five categories—national critical infrastructure (NCI), major mission critical (MMC), mission critical (MC), project essential (PE), and low risk—Reclamation has recategorized some of them in response to new research and updated results from explosives tests. In the committee's opinion, Reclamation should also consider refinements within the NCI category.

In the course of the study, the committee visited each of the five NCI dams. Providing a robust level of security for each of them is essential, and the BOR has invested more resources in protecting these dams than other facilities, which is appropriate given their importance. However, the potential consequence of a security-related failure at Folsom Dam is an order of magnitude greater than it would be for the other four NCI sites, which makes Folsom the highest priority facility within the NCI category.

Folsom Dam was built in 1956 for flood control in what was then a rural area. Over time, the surrounding area was developed and became a popular recreation site. Today, the facility includes the dam, a power plant, two reservoirs, and a series of embankments and levees. It supplies power and water to the city of Sacramento, California, and irrigation water to support a large agricultural industry. More than 700,000 people live downstream of the dam in developments located behind a series of dikes and levees, similar to the city of New Orleans, Louisiana.

To date, the effort and resources expended to improve security at Folsom Dam have been substantial. A highway that traverses the dam has been closed, and a new bridge is being built to accommodate a new road alignment that will make the dam more secure. Trails along the tops of dikes and levees remain open to the public for walking, jogging, biking, and horseback riding.

On-site security is provided by professional law enforcement officers from the Sacramento County sheriff's department under a contract with Reclamation. The police officers have received specialized security-related training under this contract. Some of the funds for this contractual arrangement were diverted from Folsom's operations and maintenance accounts to security. The contract will be in effect for 5 years, but it is not known if this arrangement will continue beyond that time. At Folsom, large construction projects, including a new spillway project being built by the U.S. Army Corps of Engineers (USACE), will be under way for the next 10-15 years. Reclamation will need to clear hundreds of contract workers through the personal identity verification (PIV) process.

Finding: Folsom Dam requires special consideration within the NCI classification owing to the magnitude of the potential consequences of a security-related failure. The level of resources required for effective security is greater at Folsom than elsewhere.

Development of Threat Scenarios

The information provided to the committee indicates that only a handful of standard threat scenarios (e.g., truck bombs, an airplane hitting a dam, the use of underwater explosives) have been assessed for individual facilities. It is easy to imagine many other plausible threat scenarios—multiple, simultaneous attacks, attacks by small bands of heavily armed individuals, or the use of insiders (through physical coercion or collaboration)—that could be evaluated for individual facilities or groups of facilities connected through SCADA systems. Even more scenarios could be developed by considering the capabilities (as opposed to the intentions) of various extremist groups. However, given the size and geographic separation of Reclamation's critical facilities, the dynamic threat environment, and Reclamation's limited resources, it is not feasible or even desirable for Reclamation to evaluate an unreasonably large number of scenarios for all of its critical facilities. On the other hand, developing any single threat scenario risks pursuing a consensus-based, most-likely scenario to the exclusion of other threats that may be less likely but more consequential if they are realized. In the absence of realistic and site-specific threat scenarios, risk assessment programs can become bureaucratic exercises. Further, because no one knows which specific threats should be defended against at each facility, strategies for the allocation of resources become less effective.

Reclamation has invested in establishing and sustaining an intelligence-gathering unit. This unit has been notified of and recorded more than 1,130 suspicious incidents at Reclamation facilities since Sep-

tember 2001. To the committee's knowledge, no intelligence-based information was incorporated into the risk management process to develop realistic threat scenarios that could be used to assess vulnerabilities for specific individual facilities. In the committee's opinion, doing so would better prepare Reclamation to defend those facilities.

Having a more robust range of plausible, site-specific scenarios would also allow a more strategic approach to the allocation of resources. It might also suggest changes in the categorization of some dams, modifications of risk mitigation projects, and a reprioritization of projects. In the end, failure to develop and evaluate more robust, site-specific threat scenarios could leave Reclamation unprepared for preventing, deterring, or responding to a malicious act.

The committee encourages SSLE staff to build on the information it has collected and consult with the various intelligence groups, such as the FBI, and other specialists to create realistic, site-specific threat scenarios for evaluation. In addition, SSLE should ask regional, area office, and facility operations staff for their input. For example, facility operators and others might role-play a group of terrorists and suggest how they would go about compromising a facility. In the committee's opinion, the incorporation of intelligence-based information into threat scenario development should improve Reclamation's capacity to protect its facilities and leverage the resources it has already invested in security.

Finding: Reclamation evaluated a very limited number of standard threat scenarios for its security assessments. Security-related intelligence has not been integrated into site-specific, realistic threat scenarios to the committee's knowledge.

Cycle for Security Assessments

The importance of conducting recurring security assessments is well understood by SSLE staff and most of the field personnel with whom the committee spoke. Reclamation plans to pattern the frequency of security assessments on the cycle used in the safety of dams program. The benefit of having a fixed schedule or cycle for conducting such assessments is that the assessments usually get done. However, the committee is concerned that if Reclamation adheres too strictly to a set timetable for assessments of security-related vulnerabilities, it risks missing some important changes and will not be able to address them in a timely way.

Dam safety issues, such as aging facilities, wear and tear on equipment, seismic design, and the like, are usually identified in a relatively static environment, and mitigation projects are then planned and scheduled for implementation. Security threats, in contrast, are continually

emerging and must be continuously monitored. For that reason, the risk to a facility from a malicious act is variable. Risk changes based on the availability and quality of intelligence information, the national threat condition, seasonal variations in reservoir conditions, the encroachment of habitation, status of the facility's maintenance, changes to the physical surroundings and facility configuration, availability and quality of security response forces, and even political pressures to compromise security-driven rules and decisions—for instance, commuters (who are also voters) might press for the reopening of roads across dams.

In short, many different factors can alter a facility's risk profile much more frequently than every 3 to 6 years. Thus the long gap between assessments not only risks failing to address significant changes in a timely way, but it also signals a management attitude that is inconsistent with the professed desire to establish a security culture within the organization. It would be better to have a less prescriptive approach that would allow security managers to conduct out-of-cycle assessments for special reasons or specific facilities.

Finding: Reclamation plans to conduct security assessments on a 3- to 6-year cycle even though security threats are continually emerging and must be continuously monitored.

PERSONNEL SECURITY

When security precautions are viewed as a system, the terrorist's potential use of insiders—through physical coercion or by collaboration—to override security components and seize control of a facility is a serious threat. Threats are also posed by disgruntled insiders who independently are capable of controlling elements of a dam's operations. An insider could be a Reclamation or water and power authority employee, or one of the many contractors who have regular access to some Reclamation facilities.

Although Reclamation managers and personnel acknowledged the threat posed by insiders, the committee was not convinced that this possibility had been fully appreciated or that effective measures to prevent or respond to it had been fully developed. For example, at one NCI site it was reported that contract workers had cut holes in fences so that they could bypass security checkpoints. It was also reported that dynamite had been found on the site, apparently left by a contract worker.

Providing a full-time escort service for uncleared contractors using government employees or guards is expensive and can be problematic. Although contractors are required to undergo the PIV process, it is not clear whether PIVs are used routinely and consistently across the BOR

regions. As currently conducted, the PIV screening process increases the time it takes to complete projects and increases their overall costs, which may, in turn, be a disincentive to use the PIV process at some Reclamation sites.

As of July 2008, the *Reclamation Manual* did not contain Reclamation-wide guidance on site access procedures for contractors. In the absence of such guidance, some area offices had developed their own procedures. At one NCI site, the area office had developed an identification and badge system that limited access to certain areas or zones of the facility to cleared individuals. The field personnel were concerned that SSLE would eventually develop guidance on its own without consulting the area offices and that by so doing, would not take advantage of the lessons learned from field experience. They were also concerned that when a policy was issued, they would have to institute a new system, even if the process in place was effective.

With numerous construction projects under way, plans and drawings for Reclamation facilities and projects are used by staff and contractors daily. The committee reviewed the *Reclamation Manual* and found it did not include guidance on safeguarding plans or limiting the number of copies in circulation.

Finding: Reclamation has not adequately addressed threats posed by insiders—Reclamation staff, facility operators, contractors—to override physical security components and take control of dam operations.

Finding: Reclamation-wide guidance on site access procedures for contractors and on safeguarding plans and drawings for construction projects has not been issued. In the absence of such guidance, some area offices have developed their own procedures.

FACILITY SECURITY PLANS

A robust facility security plan should include an integrated system with obstacles that restrict access, surveillance and intrusion detection systems, and a rapid-response force. Typically, a plan will provide defense in depth by layering security zones. For example, Zone 1, furthest from the facility, might be fenced and posted with No Trespassing signs or have security guards at key access points. Zone 2 might have intrusion detection devices and a warning system that notifies anyone entering that he or she is in a secure area. The innermost zone might have additional security features and a warning that deadly force is authorized against intruders. The rapid-response force needs to be able to act on the information provided by intrusion detection devices and to be able to use

the extra time afforded by obstacles to defeat an intruder before serious damage is done. The military has long understood that passive obstacles may delay but cannot prevent a determined opponent from gaining access to a restricted area or zone. Hence the need for a rapid-response force to confront intruders.

Security plans for individual Reclamation facilities typically incorporate access control and camera surveillance, among other things. Some plans also incorporate on-site security guards or law enforcement personnel who could respond to an incident. With few exceptions, however, such as the Hoover and Grand Coulee dams, Reclamation relies on local law enforcement entities to respond to incidents.

Although some elements of a facility security plan were visible at most sites the committee visited, there was little evidence that separate elements had been integrated to provide for a robust prevention, deterrence, and response capability. At some sites, the committee was struck by the lack of depth: If one line of physical security was neutralized, it was too likely that intruders could continue to move forward. The committee observed security gates and fencing that could be driven through by a relatively heavy truck and buildings and facilities that could be entered by scaling down nearby rock faces or by jumping fences to access unmonitored windows.

Although the committee observed some control of vehicular access across the tops of dams, ranging from total prohibition to random inspections of vehicles, there were sites where traffic flowed unrestricted. In part the different approaches were based on the identified level of risk. However, the connection between the level of risk and the mitigation measures in place was not always evident. For example, at one of the NCI sites, the road crossing the dam had been closed to all but local traffic. However, several miles away the road across another dam with an interdependent control facility was open to all vehicular traffic, making both dams vulnerable to a malicious act.

Finding: A robust facility security plan provides for defense in depth through an integrated system made up of obstacles that restrict access, surveillance and intrusion detection systems, and a rapid-response force. Although elements of a facility security plan were visible at most sites that the committee visited, the elements did not appear to be effectively integrated.

Finding: At some sites the committee could imagine threat scenarios, especially those involving insiders, that could not be countered effectively by the forces and fortifications in place. Too often facility security defenses appeared brittle and lacking in depth. If one line of facility

security was neutralized, it was too likely that intruders could continue moving forward.

Security Project Design

The design of security mitigation projects such as surveillance systems, access control, and the hardening of doors, walls, and windows is the responsibility of SSLE's security group, with technical support from the TSC. During the site visits, the committee observed several projects with design and/or installation flaws. At one site, retractable bollards installed in front of earthen structures and sensitive areas were unreliable because they relied on solar power; there were plans to fix this problem. At another site, some but not all walls and doors around an operations control room had been hardened, but an intruder could bypass the more secure doors and access the control room through a regular door. At the same facility, the staff kept the hardened doors to the control room open because conduits for electrical wires were left exposed in a room with no fire suppression system, creating a life safety hazard. Personnel at this facility clearly felt that such mistakes could have been avoided if SSLE staff had consulted with them before the project was installed. In a third instance, the design and installation of relatively simple projects was delayed because the TSC staff in Denver had other design priorities. Reclamation's field personnel believed local contractors could have designed and installed a comparable project faster and at no greater cost. Whether or not the field personnel were correct in their assessments, these discussions were indicative of the general tension between the SSLE and field personnel. The tension is fed by a lack of communication and collaboration between the Denver-based staff and the regional and area offices.

Finding: The committee observed design and installation flaws in several risk mitigation projects. The personnel at the relevant facilities clearly believed that such flaws could have been avoided if the SSLE staff had sought their input during the planning process, before the projects were designed and installed.

INCIDENT RESPONSE

A security-related incident at a BOR facility will require a response by appropriately trained and equipped security and law enforcement personnel. Reclamation depends heavily on a variety of local, state, and non-BOR law enforcement entities, as well as private security guards, for both routine security and as first responders to a malicious act.

The decentralization of U.S. law enforcement means that each Reclamation facility is located in a different jurisdiction with different laws and a unique mix of local, county, state, and federal law enforcement entities often having different communication modalities, equipment, and capabilities. Thus the interface between initial responders and the local law enforcement entities that provide follow-up to a security-related incident may differ substantially from site to site. When developing response plans for its facilities, Reclamation should therefore take into account differences in federal, state, and local laws, including those relating to the use of deadly force. The responsible parties for each facility should develop effective arrangements for working together in a crisis; such arrangements should provide for clear lines of communication and equipment that is interoperable and reliable.

Finding: Because each Reclamation facility is in a different jurisdiction with different laws and a unique mix of local, county, state, and federal law enforcement entities, the interface between first responders and those that provide follow-up will vary. Facility security plans will therefore need to incorporate distinct arrangements for cooperation among the various responders during a security-related incident.

Chain of Command

In the course of its site visits, the committee asked Reclamation personnel and other participants about the chain of command and the process for transferring authority among responders during a security-related incident. A common reply was that every potential responder had been trained in the National Incident Management System (NIMS), which is the model for a sound response to terrorism and many other incidents. This faith in NIMS may be naive, however, because the NIMS handbook clearly states that "NIMS is not an operational incident management . . . plan" (8-07 DRAFT p. 3).

When pressed for additional information on how NIMS would be implemented in specific incidents at specific locations, respondents typically referred to a chain of command order specifying that the most senior person on the scene would be in charge until relieved by someone of higher rank. However, who such people might be, where they might work (e.g., in a local, state, or federal agency), and what sorts of expertise they might possess were not well understood. The committee concluded that the coordination and transfer of authority among responders to a security-related incident could be extremely challenging.

The committee is also concerned about the highly variable and convoluted procedures for making decisions in a security-related crisis. With

multiple agencies and jurisdictions involved, the command-and-control function is critical. However, when questioned, Reclamation field personnel were generally unable to describe accurately and with confidence the specific command-and-control arrangements that would be in force. There was agreement that the manager of the facility or the area office would initially be the senior Reclamation person on the scene, but it was not well understood what the relationship might be between federal staff and local law enforcement. How (or even if) the regional director, the SSLE director, or the RSAs would take part in command, control, and decision making was also not clear. This lack of clarity in roles and responsibilities would be exacerbated, in accord with NIMS, if other federal agencies were called in to help.

Following a number of investigations into the problems and circumstances surrounding damage to New Orleans in the aftermath of Hurricane Katrina, the American Society of Civil Engineers (ASCE), at the invitation of USACE, undertook an independent investigation of what went wrong. In its summary, ASCE listed 10 "calls to action." Number 6 was, "Put someone in charge." ASCE added to this, saying that "no complex program or system can be successful without good leadership, management, and someone in charge" (ASCE, 2007, p. 79). Reclamation needs to heed this advice. The response plan for each facility should clearly describe the evolution of the chain of command and the transfer of leadership responsibility during a security-related incident. Response plans should also say who should be in charge during each phase of the response—that is, who would be the senior person on the scene initially and as events unfold.

Finding: Specific guidelines for command, control, and decision making at individual sites enable an effective response to a security-related incident. At Reclamation, guidance for those responsibilities was unclear, and procedures were not well understood by staff.

Communication During a Response

Communication is critical for an effective response to a security-related incident, but it can be difficult even when responders share a language, equipment, and technologies. If personnel from multiple law enforcement entities are using equipment that is not interoperable or if they are communicating on different channels, the flow of critical information about the incident and the response will be hindered. The committee observed that some communication equipment and technologies used by Reclamation personnel and contractors were not interoperable with those used by local law enforcement and other responders and that different radio frequencies and channels were used. This situation suggests that BOR should

make sure that its staff, operators, and contractors have the appropriate equipment to communicate with the local law enforcement groups that would respond at each site or it should work toward some standardized Reclamation-wide communication modes. Reclamation-wide protocols for radio communications during an incident are also needed.

The committee also heard about single-point failures of communication systems that could affect incident response. For example, in one instance, lightning struck an electrical tower and knocked out power to a large area, including a Reclamation facility. No replacement transformer was available locally. Reclamation staff were called out to guard their facilities until a generator could be found, shipped, and made operational.

In some rural or remote areas, cell phone coverage is limited. Microwave and satellite phones may be the primary means of communication and for the operation of SCADA systems. If these systems are rendered inoperable, there is no backup communication technology. This is especially problematic where centralized SCADA systems control a group of dams and the loss of one antenna site can disable connectivity to several other sites. In one region, actions were taken to mitigate the risk of SCADA system failure, but it is not clear whether other regions have taken similar mitigation actions.

Finding: Good communication is critical for an effective response to a security-related incident. The committee observed that some communication equipment and technologies used by Reclamation and other federal, state, and local law enforcement and security organizations were not interoperable and would hinder communication among responders.

Finding: Certain communication technologies used in rural and remote areas are subject to failure caused by weather and related events and may not be reliable during a security-related incident.

Use of Deadly Force

The circumstances under which security and law enforcement personnel are permitted to employ deadly force is a major concern. Legally binding guidance on how and when deadly force is appropriate for a security-related incident appears to be inconsistent, nonexistent, or ambiguous because of the overlap of legal jurisdictions, uncertainty over the divide between security and law enforcement, the absence of operational guidance, and no clear chain of command.

In the United States, the standard for the use of deadly force by police officers (what in military terms is referred to as rules of engagement) to enforce the law is clear: Officers may use it to (1) protect themselves and

innocent bystanders from imminent threats of serious injury or death (often referred to as the defense-of-life rule) or (2) apprehend fleeing suspects when they have probable cause to believe that the suspect has committed a crime involving the infliction or threatened infliction of serious injury (often referred to as the violent-fleeing-felon rule). Federal (as opposed to local) law enforcement policies for the use of deadly force essentially limit federal officers to the defense-of-life rule.

Discussions with Reclamation law enforcement officers and contract security personnel indicated that the individuals who are authorized to carry firearms have a sound understanding of the defense-of-life rule. What is not clear, however, is how this rule might apply in security-related incidents. For example, committee members described to field personnel a scenario involving a vehicle- or watercraft-borne improvised explosive device (IED) attack that might substantially damage either a dam or some attendant facility. BOR law enforcement and security personnel believed the officers on the scene would not be authorized to use deadly force to stop the vessel because the threat was to property, not people. This opinion about the appropriateness of deadly force is consistent with standard law enforcement training. However, it might not be appropriate for dealing with terrorist attacks or other security-related incidents.

Although a Reclamation law enforcement or security officer cannot be certain of the explosive yield of any specific vehicle- or water-borne IED (or, for that matter, whether a suspicious vehicle or watercraft is actually undertaking an attack), large explosives may well be able to injure or kill people who are a substantial distance from the point of detonation. In addition, Reclamation security and law enforcement personnel cannot know with certainty whether an attack would damage the facility to the point where lives would be endangered. If a dam were to fail, for example, the lives of all individuals in the inundation plain below it would be threatened. Considerations of this sort are not typically contemplated when police and security trainers instruct officers about deadly force decision making, but it struck the committee that they should be in the case of armed Reclamation law enforcement and security personnel.

Finding: The objectives and operating procedures for law enforcement are different from those for security. The legislation giving Reclamation law enforcement authority does not address issues of antiterrorism or security, nor does it permit Reclamation to hire its own law enforcement personnel.

Finding: The distinction between law enforcement and security within Reclamation is not clear, and the resulting ambiguity has raised issues regarding the use of deadly force during a security-related incident.

A related concern involves the types of ammunition in use. One aspect of this has to do with the fragility of equipment inside facilities. Discussions with selected SSLE personnel indicated that the use of standard ammunition in specific portions of a facility could substantially compromise the integrity of critical equipment. It was not clear, however, that this was common knowledge throughout the SSLE or among the various on-site security and law enforcement entities at BOR facilities. Nor was it clear that the various secondary and tertiary responders in local, state, and federal law enforcement agencies were aware of this issue. Discussions with one person in the SSLE disclosed that members of at least one responding entity were aware of the issue and understood that frangible bullets would be superior to standard ammunition should they need to mount a counterterror operation in specific areas of the facility.

Finding: The use of standard ammunition in some parts of some Reclamation facilities could substantially compromise the integrity of critical equipment. It was not clear if this was common knowledge throughout SSLE or among those security and law enforcement entities that would respond to a security-related incident.

EXERCISES AND TRAINING

As noted in Chapter 2, tabletop, functional, and full-scale exercises are an important training tool and method for identifying problems or limitations in response plans and processes and fixing them in advance of a security-related event. Reclamation routinely conducts tabletop and functional exercises in conjunction with its safety of dams and emergency management programs. It is not clear how many such exercises have been conducted for security-related processes and functions.

Three full-scale exercises specifically related to a security incident have been conducted since the 9/11 attacks. The committee's understanding is that owing to limited resources the only Reclamation field staff who participated in these exercises were the regional and area office managers responsible for the specific facility where the exercise was being conducted. One of the most important products of a full-scale exercise is an after-action report that can be used to improve processes not only at the particular facility but at other facilities as well. Such reports could be particularly useful to regional and area office directors who did not participate in the exercise. They could compare the findings in the report to their own procedures and, if similar problems had been identified, proactively fix those problems at their facility. This might be an especially important capability for area office managers who would be responsible for the initial response to a security-related incident at their facilities. By disseminat-

ing the after-action report to a broader audience, the resources invested in full-scale exercises can be leveraged to improve security throughout Reclamation. However, several area office managers reported they had never seen the after-action reports for the Grand Coulee or Flaming Gorge exercises. Because such reports may contain some sensitive information, procedures will be required to ensure that when the reports are not in direct use, they are kept in a secure place and not left in plain view.

As noted in Chapter 2, full-scale exercises require a substantial investment of time, expertise, and resources. The committee was told of an instance in which the FBI approached one of the area offices about conducting an exercise at a Reclamation dam using FBI funding. However, the proposal was not approved by the SSLE. While the committee recognizes that there may be many reasons for such a decision, it is also important for the SSLE to take advantage of opportunities to leverage its resources and improve its preparedness. If a similar opportunity should arise in the future, the SSLE should give it careful consideration and make a concerted effort to collaborate with the outside entity. If an arrangement cannot be worked out, the reasons for this should be clearly communicated to field staff.

The various security and law enforcement entities at each critical facility should also train appropriately for the specific challenges they would be likely to face in the event of a malicious act. Some facilities appeared to have matched training to the threat environment, while others had not. At one facility, for example, the members of the tactical response group understood that their primary mission in the event of a major incident would be to secure the facility and then wait for backup support to arrive; the group was to take action only in extreme circumstances. Despite this understanding, they trained regularly for hostage rescue scenarios but had yet to do a site survey of the interior of the facility to familiarize themselves with its layout, something that would be tremendously useful if an incident were to occur inside the facility.

The use of red teams to test Reclamation's preparedness, especially as it relates to the counterintelligence function of the law enforcement administrator, should be seriously considered by senior management at Reclamation.

Finding: Training exercises are important to ensure that when personnel from multiple government and law enforcement entities respond to a security-related incident, all of the key players understand the procedures for command and control and for the transfer of authority as events unfold. Training exercises need to be designed to test site-specific, realistic scenarios and to be aligned with the responsibilities of the responders.

INTELLIGENCE GATHERING AND DISSEMINATION

A culture within intelligence communities resists the sharing of information, limiting access to those whom it deems need to know. An inflexible commitment to the need-to-know doctrine appears to be inhibiting intelligence sharing between the SSLE and Reclamation's field personnel, who would be the first to respond to suspicious activity or a malicious act at their facility.

Security-related information for Reclamation's facilities comes from a number of sources, including the FBI, SSLE's LEA, operations personnel, local law enforcement, and sometimes the community at large (say, the manager of a boat rental business). Gathering information from many sources and analyzing it to determine if an action is needed requires good internal and external working relationships and partnerships and effective communication systems.

Within Reclamation's security structure, the LEA in Denver is the central point for collecting security-related information, which it inputs into a database of security-related incidents. The RSAs serve as liaisons between Denver headquarters, their regional and area offices, facility personnel, and local law enforcement. Although the RSAs meet with intelligence counterparts in the field through the JTTFs and perhaps others, there are restrictions on the information the RSAs can convey to other BOR operating personnel, including the RSOs, at the various facilities. Use of the database is also restricted.

The rationale for restricting the dissemination of classified information is clear: Some area offices are not equipped to receive or handle classified information and some operating personnel do not have the appropriate security clearances. However, much of the information on suspicious activities or incidents is not classified; rather, it is deemed "sensitive," a more ambiguous characterization. Although an RSA is expected to relay sensitive information to the LEA in Denver, sensitive information gathered and analyzed by the LEA is not consistently shared with an RSA even if the information originates in his or her region at the local level. It appears that the LEA only rarely shares intelligence-based information across regions. Thus the RSA in Region A may never formally hear about an incident in Region B even if the information might be helpful in identifying similar incidents or patterns of activity in Region A. Incidents and reports on the activities of suspect individuals or representatives of suspect groups often are not passed on to neighboring facility managers, again on the basis of the information's sensitivity and inflexible need-to-know limitations. This lack of communication and restricted information sharing frustrates conscientious operating officials, who feel they are being denied information that would allow them to meet their security-related responsibilities. The holding back of information by the SSLE also undercuts the authority and

credibility of the RSAs and makes it unnecessarily difficult for the RSAs to build trust and good working relationships with Reclamation field personnel and local officials.

Effective intelligence gathering requires that people at the local level (Reclamation personnel, water and power authority staff, law enforcement, and the public) be alert to suspicious activities and behaviors and that they have a means to communicate that information to the RSAs or other Reclamation personnel. The SSLE is posting signs that encourage people who see something to say something and provides an 800 number to call and an e-mail address. A Reclamation-wide policy on reporting suspicious activity has been drafted but has not yet been issued.

The committee repeatedly heard that operations personnel who have forwarded information of potential intelligence value to an RSA or the LEA seem only rarely to be later told if the information they provided had been useful, and if so, how? Consequently, operations personnel view communication with SSLE in Denver as a one-way street. Some quietly admit that they no longer bother to report on or forward information about suspicious activities since doing so appears to be of no avail. This attitude, which is due to the lack of feedback, could mean that a threat to Reclamation facilities is not identified in time to take preventive action.

Finding: An inflexible commitment to the need-to-know doctrine inhibits the sharing of intelligence-based information among SSLE staff in Denver, the regional special agents, and the area office personnel who might be in the best position to deter some threats and who would be the first responders to an incident.

Finding: Field personnel and others who have reported potentially valuable information about suspicious activities to the SSLE in Denver only rarely receive feedback on how or even if the information was used. As a consequence, some field personnel view security-related communication as a one-way street and are reluctant to report information about suspicious activities since their effort appears to have no effect.

WORKING RELATIONSHIPS

With a largely decentralized organizational structure and a heavy reliance on partnerships and contractors, Reclamation is fundamentally dependent on internal and external collaboration to achieve its mission of delivering power and water in an environmentally sound manner. Collaborative working relationships, in turn, are based on effective communications and trust.

Effective communication involves transmitting information in a manner that evokes understanding. It requires more than a good presentation or a dynamic messenger; effectiveness has to do with the quality of the message, the credibility of the information, and the deliberations that ensue. Effective communication within an organization involves managing the flow of information among the various working groups and partners to ensure that those who need to know and who can best act on the information are brought in to the process at a sufficiently early stage to provide insights that can produce a better outcome or a better response. Typically, the more open the process, the more likely it is that errors in fact or in methodology will be uncovered. Classified information may not, of course, be freely shared and is an exception to an open flow of information (NRC, 2004).

Trust is important to the success of working relationships. Building trust is a complex process because it is difficult to establish and easy to destroy. Although many positive transactions are required to build trust, a single instance of poor communication can be interpreted as deception, and the hard-won trust is lost (NRC, 2004).

Since 1994, many of the BOR's functions have been decentralized and directed by regional and area office managers (NRC, 2006). A decentralized organizational structure is not optimal for establishing a security program. A centralized approach to threat and risk assessment, policy guidance, and intelligence analysis is more suitable. If the security program and a culture of security are to become embedded at Reclamation, good working relationships, effective communications, and trust must first be developed within the organization.

Because the security program is relatively new and has not yet been fully integrated into the culture and mind-set of BOR personnel, many of them view it as necessary but do not welcome it. Owing partly to its centralized structure, the SSLE and its personnel are viewed from the field as bureaucratic, generally uncommunicative, and outside Reclamation norms and traditions. Some directors and managers at the regional and area offices resist surrendering their delegated authority, which collides with efforts to implement Reclamation-wide security policies, plans, and programs. The tension between SSLE and the field organizations obstructs the development of a more robust security program and culture.

The sources of this internal tension go beyond SSLE's organizational structure to include managerial actions and staff behavior. As noted previously, when designing and implementing security-related measures, the SSLE appears to have acted unilaterally with little or no input from field personnel. The lack of interaction during the planning stage of these projects has led to design flaws that might have been avoided if field personnel had been consulted. In addition, it signals that SSLE does not

want or value input from the regional or area offices, which leads to animosity and distrust. The restricted sharing of intelligence-based information from SSLE's Denver headquarters to and across regions and the lack of feedback when field-based information is sent up the line to SSLE also damages working relationships and, more important, Reclamation's ability to respond to security-related threats.

Reclamation's regional, area, and local managers have developed and depend on a network of working relationships with local security and law enforcement entities, with water and power districts, and others. In some instances, SSLE staff have bypassed regional and area offices and interacted directly with law enforcement and with the water and power districts. The regional and field managers are concerned that such actions jeopardize the relationships that their staffs have nurtured and undercut their credibility with their partners. The end result, again, is tension and distrust between regional and area office managers and the SSLE.

As noted in Chapter 1, to improve security Reclamation must also partner with the USACE, the Department of Energy, state departments of transportation, and other organizations to mitigate vulnerabilities of facilities that are interdependent with Reclamation facilities but not under Reclamation's direct control. The sharing of information—for example, the risk assessments conducted by California state agencies for some of Reclamation's dams—would also improve security. Partnering with these outside organizations requires good working relationships based on trust and communication.

Finding: With its largely decentralized organizational structure and heavy reliance on partnerships and contractors, Reclamation is fundamentally dependent on collaboration within and among organizations to achieve its mission. Imposing a centralized security program on a culture that is accustomed to distributed program management and authority has resulted in tensions and ineffective working relationships between the SSLE staff in Denver and the staff of regional and area offices.

Finding: Sound working relationships are based on effective communications and trust. Managerial actions and the behavior of SSLE's Denver-based staff have in some cases created distrust among the regional and area office staff that is damaging to internal working relationships and limits the effectiveness of the security program.

EXPERTISE

Immediately after the 9/11 attacks, as Reclamation was creating the SSLE, positions were primarily filled by transferring people from other sec-

tions in Reclamation and the DOI who may not have had much security-related experience. In the years since, Reclamation has made an effort to recruit personnel with security and law enforcement backgrounds and to upgrade the organization's overall security-related knowledge, skills, and abilities.

Recruiting people with the required competencies is not an easy task. Attracting younger workers to the federal government can be difficult, because recent college graduates do not view the federal government as an employer of choice (PPS, 2006). More experienced law enforcement officials or personnel with security-related backgrounds may be attracted by the federal government's benefits package and relative job security. However, the federal hiring process is cumbersome, confusing, and slow, and many who do apply for positions drop out of the process to take other jobs (MSPB, 2004). The challenge of recruiting new people to fill positions in Reclamation is further exacerbated by the high cost of living in areas like Sacramento, California, and the remoteness of many facilities. One of the earlier reviews of Reclamation's security program noted that the Department of Energy's pay scale was significantly higher for some similar positions. In addition, for some security or law enforcement positions there is no obvious career ladder with the possibility of future promotions, increased salary, and more complex assignments.

When recruiting new staff is problematic, the training of current staff becomes especially important to ensure that the appropriate skills are present in the organization. Staff with engineering or law enforcement expertise can be singled out to receive specialized training in security-related issues, practices, and procedures.

Because Reclamation relies on good working relationships with internal staff and outside partners for effective operations, SSLE staff in particular need good communication, negotiation, and team-building skills. Training current staff in these skills could help to improve internal and external working relationships and the overall effectiveness of the security program. When recruiting new personnel, special emphasis should be given to these skills in job descriptions and during the interview process.

Finding: Although the SSLE's Denver-based staff may have the technical skills necessary to carry out their job responsibilities, they have not in general displayed the communication, negotiation, and team-building skills needed for the sound working relationships that are critical to Reclamation.

REFERENCES

American Society of Civil Engineers (ASCE). 2007. *The New Orleans Hurricane Protection System: What Went Wrong and Why.* Reston, Va.: ASCE.

Merit Systems Protection Boards (MSPB). 2004. *Managing Federal Recruitment: Issues, Insights, and Illustrations.* Washington, D.C.: MSPB.

National Research Council (NRC). 2006. *Managing Construction and Infrastructure in the 21st Century Bureau of Reclamation.* Washington, D.C.: The National Academies Press, pp. 4-5.

NRC. 2004. *Investments in Federal Facilities: Asset Management Strategies for the 21st Century.* Washington, D.C.: The National Academies Press.

Partnership for Public Service (PPS). 2006. *Back to School: Rethinking Federal Recruiting on College Campuses.* Washington, D.C.: PPS.

4

Future Plans

In addition to evaluating Reclamation's security-related processes, working relationships, and expertise, the committee was asked to evaluate Reclamation's future plans for its security program. In the nearly 7 years since the September 11, 2001, attacks, Reclamation has had to develop a security program starting from almost nothing. While it has made significant progress in doing so, some fundamental issues need to be resolved for Reclamation to develop a culture of security as strong as its culture of dam safety—that is, one in which the policies, practices, and procedures for dam security are well developed and reflected in Reclamation's decision making and routine operations. Developing a culture of security and a program that is sustainable over the long term will require the following:

- Senior management support and commitment,
- Adequate resources,
- Performance measurement and evaluation,
- A system for capturing and disseminating lessons learned, and
- A vision and a long-term plan for a sustainable program.

Chapter 4 focuses on these elements and the committee's observations and findings related to Reclamation's plans for its security program.

SENIOR MANAGEMENT SUPPORT AND COMMITMENT

Building commitment and support for the security program is primarily the responsibility of the senior executives within Reclamation—the commissioner, deputy commissioners, regional directors, and the director and program managers of the SSLE. Support, commitment, and leadership should begin with the commissioner and the deputy commissioners and continue uninterrupted down through the regional, program, and area office directors to the facility operators and line personnel. Reclamation's senior managers are responsible for establishing the vision and objectives for the security program, establishing Reclamation-wide policies and procedures, determining priorities for resource allocation, selecting personnel in key positions, and communicating why a security program is critical to achieving Reclamation's mission. Establishing metrics for progress in achieving security-related objectives and outcomes, assigning responsibilities clearly to key individuals, providing adequate resources to meet program objectives, and holding their staff accountable for results are also responsibilities of senior managers.

The federal government's Office of Personnel Management (OPM) has developed a set of executive core qualifications (ECQs) needed to achieve a federal corporate culture that motivates for results, serves customers, and builds successful teams and coalitions within and outside the organization (OPM, 2007). The ECQs defined by the OPM include these:

- *Leading change* . . . the ability to bring about strategic change, both within and outside the organization, to meet organizational goals [and to] establish an organizational vision and implement it in a continuously changing environment.
- *Leading people* . . . the ability to guide people to meet the organization's vision, mission, and goals [and to] provide an inclusive workplace that fosters professional development, facilitates cooperation and teamwork, and supports constructive resolution of conflicts.
- *Results driven* . . . the ability to meet organizational goals and customer expectations [and to] make decisions that produce high-quality results by applying technical knowledge, analyzing problems, and calculating risks.
- *Business acumen* . . . the ability to manage human, financial, and information resources strategically.
- *Building coalitions* . . . the ability to build coalitions internally and with other federal agencies, state and local governments, nonprofit and private-sector entities, foreign governments, or international organizations to achieve common goals.

The committee devoted significant time and energy to observing, discussing, and evaluating senior management's understanding and commitment to the security program. Committee members met with senior executives and managers at Reclamation's Washington, D.C., office and its Denver headquarters, at regional and area offices, and at individual sites. It was clear to the committee that Reclamation's personnel at all levels are committed to the dam safety and emergency management programs. The relationship of these programs to the achievement of the BOR's mission of delivering water and power seems to be consistently communicated from the top down through all levels of the organization and is well understood by all.

In contrast, discussions on dam security did not convey the same level of support and commitment from senior management or field personnel. Nor was the link between security and mission achievement consistently recognized or communicated. Personnel at all levels clearly understand that the NCI facilities and some other highly visible dams constitute attractive targets for terrorists, and they support actions to protect those facilities. However, the commitment to providing security for the majority of Reclamation's dams was not consistent. Because many dams are not icons, are located in rural areas, or are smaller, they seem less likely to be targets of terrorists, which has led to thinking "it won't happen here." In some instances, staff clearly felt other priorities were higher than security, and they resented the redirection of resources from other program areas to security.

SSLE's director and program managers understand the security program's purposes and requirements. However, the organizational and communication issues described in Chapter 3 have limited the effectiveness of SSLE staff in helping to develop a culture of security.

At the regional offices, the committee observed a range of attitudes regarding the need for a robust security program, from committed to indifferent to resentful. Often the attitude exhibited by a regional director was reflected by area office managers and facility operators. Frustration and confusion were most evident among those area office managers who were clearly committed to providing security but who reported to regional office directors who were not as committed.

Finding: Creating an effective security program and a culture of security requires the dedicated support and commitment of Reclamation's managers at all levels of the organization. Currently, such support and commitment are uneven. Some managers clearly understand the link between Reclamation's mission and security, and they are spearheading efforts to implement effective security procedures and programs. Others

regard security as an unwelcome intrusion into other activities and resent the redirection of resources from other activities to security.

Finding: Building commitment and support for the security program is primarily the responsibility of Reclamation's senior executives—the commissioner, deputy commissioners, and regional directors and the director and program managers of the SSLE Office.

RESOURCES

An effective security program must be staffed with enough people possessing the necessary competencies to carry out assigned tasks and must be funded accordingly. Reclamation is attempting to operate a security program to protect 450 facilities distributed across 17 states with fewer than 50 full-time-equivalent positions. The responsibilities of this group include developing Reclamation-wide policies and operating procedures, conducting security assessments, managing risks, identifying risk mitigation projects and prioritizing them across an inventory of facilities, conducting background checks on staff and contractors, designing and implementing physical security improvements, identifying and analyzing suspicious and criminal activities through liaisons with other federal agencies and local law enforcement, developing security response plans, conducting exercises, and responding to malicious acts. Reclamation's field personnel and its partners also participate in some aspects of the security program, which leverages the resources available to the SSLE. Nonetheless, a situation in which each regional special agent (RSA) is responsible for an area covering portions of between three and nine states suggests that additional staff resources are required if the SSLE and Reclamation are to meet their security-related responsibilities effectively.

Current funding is inadequate to hire additional staff and to implement other activities that are needed to improve the security program. Reclamation has a backlog of risk-mitigation projects that have not been implemented, in part because there are not enough resources for designing and installing them. Very few full-scale exercises have been conducted, also, in part, because of resource limitations. Furthermore, additional training for SSLE staff in communication, negotiation, and other behavioral skills is required to develop the sound working relationships that are fundamental to Reclamation's activities.

Reclamation has attempted to leverage its available funding by making some security-related operation and maintenance costs fully reimbursable. This initiative, however, has created additional tension between the BOR and some of its stakeholders, particularly water and power authorities. Designating projects that benefit a specific set of stake-

holders as reimbursable is a well-established and accepted procedure in Reclamation and on the part of its stakeholders as well. However, since security-related projects also provide benefits to the public at large, it is not unreasonable for Reclamation's partners to object to fully funding security guards or other activities that also benefit the general public.

Reclamation's dam safety program also seeks to protect the general public. However, some dam safety projects are partially reimbursable: Reclamation pays for 85 percent of the project, and a stakeholder who benefits from the project pays 15 percent. Criteria have been developed for determining which dam safety projects are partially reimbursable. The dam safety program may serve as a model from which to develop criteria, a process, and a percentage for reimbursement of the costs of some security-related operations and maintenance activities.

Whatever process is used to resolve the issue of reimbursability for security-related projects, the current allocation of resources—number of staff, expertise, funding—is not sufficient, in the committee's opinion, to operate and sustain a program for protecting Reclamation's assets and people. Continuing to redirect funds from other programs will undermine other Reclamation programs and the condition of its facilities. However, from its discussions with senior Reclamation managers responsible for the security program and the briefings it received from them, the committee found the managers apparently reluctant to fight for additional resources and funding.

Finding: The resources—number of staff, expertise, funding—currently available for Reclamation's security program are not sufficient to operate and sustain an effective program.

Finding: Security improvements benefit the public at large and are not limited to specific set of stakeholders. Reclamation's proposal to make some security-related costs fully reimbursable causes tension with its stakeholders. The safety of dams program, in which reimbursable project costs are split between Reclamation and its stakeholders, may serve as a model for developing criteria, a process, and a cost-sharing percentage for reimbursing the costs of some security-related operations and maintenance activities.

PERFORMANCE MEASUREMENT

In the years since the passage of the Government Performance and Results Act of 1993, measuring the outcomes of federal programs has become an established and accepted process. Key components of a performance measurement system include these:

- Clearly defined, actionable, and measurable goals that cascade from organizational mission to management and program levels to individual performance;
- Cascading key performance indicators that can be used to measure how well mission, management, program, and individual goals are being met;
- Established baselines from which progress toward attainment of goals can be measured;
- Accurate, repeatable, and verifiable data; and
- Feedback systems to support continuous improvement of an organization's processes, practices, and results (outcomes) (FFC, 2004).

Performance measures help to identify where objectives are not being met or where they are being exceeded. Managers can then investigate the factors or reasons underlying the performance and make appropriate adjustments. Ultimately, an effective performance measurement system should inform decisions about the allocation of resources within an organization (FFC, 2004).

As noted in Chapter 1, Reclamation has established elements of a performance measurement system in response to the OMB's PART evaluation process. The stated objective of Reclamation's site security effort is to reduce security-related risks through a combination of preparedness, prevention, protection, and response. The outcome is measured as the number of assets that are rated high risk. Changes in the risk rating will be determined over the long term as security improvements are implemented and risk assessments are repeated (OMB, 2007). Table 4.1 describes the performance measures that are being tracked.

These measures represent the start of a performance measurement system for Reclamation's security program. However, the actual measures focus on the risk assessment element and do not address law enforcement, intelligence gathering and dissemination, training and exercises, protection maintenance, or incident response.

The committee did not ask Reclamation managers specifically about their future plans for a performance measurement system, and it may be that additional measures are being developed by Reclamation or by DOI's OLESEM. In all events, the system should link directly to Reclamation's mission. For example, a stated goal of the security program might be to ensure that there are no serious disruptions to the delivery of power and water as the result of a malicious act. The program objectives would include preventing, deterring, mitigating, or responding to malicious acts. The performance measures developed could be used to measure the mitigation actions taken.

TABLE 4.1 Performance Measures for Reclamation's Site Security Effort

Performance Measure	Description
Cost per active background investigation	Tracks the efficiency of the background investigation and national security processes, including the ability to implement and maintain electronic methodologies for completing and submitting background investigation forms, verifying the status of investigations and clearances, and maintaining personnel security records.
Number of updated regional threat assessments	Tracks whether threat assessments are updated annually in each of the five regions and coordinated with state, local, and other federal entities.
Number of periodic security risk assessments conducted annually on critical or project-essential facilities	Tracks progress in assessing risks and identifying protective measures needed at critical facilities.
Percentage of risk assessment recommendations that have been completed	Tracks implementation (funding, installation, and operation) of individual protective measures identified in the risk assessment process.

Developing effective measures for all aspects of Reclamation's security program will be difficult. For example in reviewing the FBI's intelligence program, the OMB concluded as follows:

> It is difficult to define outcomes for a program that produces intelligence. In some cases, good intelligence analysis will lead to a physical outcome, such as a terrorist attack that is averted or a foreign intelligence penetration that is avoided, but this is not always the case. Productive and useful analysis may merely serve to enhance the government's body of knowledge on a particular topic. (OMB, 2008a, pp. 7 and 8)

Measuring for deterrence and response, in contrast, might involve tracking suspicious incidents using Reclamation's database and tracking the actions taken to investigate and respond to them. The National Park Service Police, for instance, tracks the number of incidents that pose a serious potential threat to selected national monuments. As noted by the OMB,

> the utility in this measure is not in tracking the total number, but in monitoring (and responding to) the types of incidents, when they occur, and possible trends. This output measure is used as a proxy outcome measure because measuring the desired outcome (i.e, undamaged national monuments) would be both self-evident and of little use to managers. If

> a national icon were attacked, a PART target would be the least of USPP concerns. More relevant for managers is tracking the number of incidents that pose potential threats and working to understand why those incidents occur. (OMB, 2008b, p. 2)

The number of tabletop, functional, or full-scale exercises conducted, the number of identified areas requiring improvements, and the percentage of improvements implemented might also be tracked to evaluate response capability.

In developing a more complete set of measures for its security program, Reclamation could begin by looking at the performance measures used by similar programs of other federal or quasi-federal agencies, including the Federal Protective Service, USACE, the Tennessee Valley Authority, and the Western Area Power Authority.

Finding: Reclamation has developed some performance measures for evaluating the risk mitigation component of its site security program. Additional measures are needed to evaluate processes related to deterrence of and response to security-related incidents.

METHODS FOR CAPTURING, DISSEMINATING, AND IMPLEMENTING LESSONS LEARNED

A lesson learned has been defined as "knowledge or understanding gained by experience," both positive and negative (GAO, 2002). Lessons learned programs are established to identify which actions or procedures worked and which did not work in a particular situation so that successes can be repeated and failures avoided. The U.S. General Accounting Office (now the Government Accountability Office) has stated that

> use of lessons learned is a principal component of an organizational culture committed to continuous improvement. Lessons learned mechanisms serve to communicate acquired knowledge more effectively and to ensure that beneficial information is factored into planning, work processes, and activities. Lessons learned provide a powerful method of sharing good ideas for improving work processes, facility or equipment design and operation, quality, safety, and cost-effectiveness. (GAO, 2002, p. 13)

Most formal lessons-learned processes include a searchable lessons-learned database, a method using subject experts to verify the correctness and applicability of the lessons submitted, and a process that can disseminate lessons learned to the appropriate users. Dissemination may also be accomplished by incorporating lessons learned into policies, guidelines,

or processes through training and seminars, meetings, and conferences or through publications in the form of alerts, newsletters, and the like. Less-formal programs may simply send documents such as after-action reports from a full-scale exercise or from important events, such as errors, accidents, and near misses, to managers and staff who could benefit from them.

Tabletop and functional exercises or other forms of simulation could also be vehicles for developing lessons learned. Lessons can also be learned from other organizations that have security programs deemed to be excellent. A visit to such an organization might include on-the-spot discussions of that organization's experiences in developing its security program. Reclamation personnel visiting these organizations might also hold after-visit, in-depth discussions of the security-related activities and processes they observed.

Reclamation does not appear to have a process in place to collect and disseminate lessons learned or to use them for making appropriate changes in policies and procedures. Such a process could be especially valuable in a decentralized organization, where the staff does not regularly meet to share information. Reclamation might consult with other federal organizations that have well-established lessons-learned programs, including the Department of Energy,[1] the Aviation Safety Reporting System (housed at Battelle), the Army's after-action review, the U.S. Navy's Aviation Training Exercise program (lessons learned are included in after-action "hot wash-ups"), and NASA's astronaut training program.

Finding: Lessons-learned processes can be useful for sharing experience-based information in an organization and for continually improving organizational processes, knowledge, and standards. Sources of lessons learned include after-action reports from training exercises, other forms of simulation, and other organizations.

Finding: Reclamation's security program does not appear to have a formal lessons-learned program in place. Where after-action reports followed major exercises, they were not disseminated to all the regions or the area offices that could have benefited from knowing the exercise results.

A VISION AND A LONG-TERM PLAN FOR A SUSTAINABLE PROGRAM

Vision and leadership are crucial for all aspects of an organization's activities. Typically, an organization's senior executives establish the vision

[1]DOE's lessons-learned Web site can be accessed at http://tis.eh.doe.gov/ll.

based on the organization's mission, set goals and priorities, and then communicate the vision and implementing strategies to the staff and the organization's stakeholders (GAO, 1998). Mission and vision statements and plans are all important because they are meant to inspire and motivate employees and stakeholders alike to meet the organization's goals.

As stated on its Web site, the mission of the Bureau of Reclamation is to "manage, develop, and protect water and related resources in an environmentally and economically sound manner in the interest of the American public." Reclamation's Vision Statement reads as follows:

> Through leadership, use of technical expertise, efficient operations, responsive customer service and the creativity of people, Reclamation will seek to protect local economies and preserve natural resources and ecosystems through the effective use of water.

The commissioner's plan for how Reclamation will attain its vision includes the following:

- Directing our leadership and technical expertise in water resources development and in the efficient use of water through initiatives including conservation, reuse, and research.
- Protecting the public and the environment through the adequate maintenance and appropriate operation of Reclamation's facilities.
- Managing Reclamation's facilities to fulfill water user contracts and protect and/or enhance conditions for fish, wildlife, land, and cultural resources.
- Working with Reclamation's customers and stakeholders to achieve mutual objectives.
- Assisting the secretary in fulfilling Indian Trust responsibilities.
- Implementing innovative, sound business practices with timely, cost-effective, measurable results.
- Promoting a culturally diverse workforce that encourages excellence, creativity, and achievement.

Reclamation has also outlined four overarching goals that emphasize its mission to deliver water and generate power while addressing other water use requirements and planning for future water needs to avoid crisis and conflict:

- Ensure the reliable delivery of water under Reclamation contracts.
- Optimize power generation, consistent with project purposes.
- Incorporate other considerations, such as recreation, fish and wildlife, environment, and Native American trust responsibilities, into our water and power operations.

- Identify and plan for future consumptive and nonconsumptive water supply needs by identifying unmet needs in the next 25 years.

None of the statements above explicitly addresses the security of Reclamation's facilities or its people. Protecting the public is mentioned in conjunction with the adequate maintenance and appropriate operation of Reclamation's facilities, but it reflects a dam safety perspective as opposed to a security perspective.

If security were a well-established program embedded within Reclamation's culture, the lack of an explicit reference to it in Reclamation's mission, vision, and goals statements might not be significant. After all, there is no direct mention of emergency management in the statements above, yet emergency management is clearly embedded in Reclamation's programs and culture. However, security is a relatively new program that is not consistently supported by Reclamation personnel. The failure to mention security explicitly in the mission statement, the vision, plan, or overarching goals signals that it is not a priority within Reclamation and conveys a lack of support and commitment from senior management.

Reclamation does not appear to have a plan for creating a robust, mature, and sustainable security program. When asked about their goals for the security program, senior managers focused on tactical issues such as addressing the backlog of identified risk mitigation projects, finding ways to lower the costs of site security guards, and periodically conducting threat assessments and training exercises. Strategic issues, such as how security is to be embedded in Reclamation's culture and how regional security coordination is to be improved, were not identified.

Finding: Among their other objectives, organizational mission and vision statements, plans, and goals are meant to inspire and motivate employees and stakeholders. Typically, they are driven by an organization's senior executives and reflect their priorities and values. Infrastructure security does not appear explicitly in Reclamation's mission statement, vision, plan, or goals. The failure to mention it conveys the idea that infrastructure security does not have the support and commitment of senior management, nor has it been given priority.

Finding: Reclamation does not appear to have a plan for a security program that is robust, mature, and sustainable. When asked about their goals for the security program, senior managers focused on tactical issues. Strategic issues, such as how security is to be embedded in Reclamation's culture and how regional security coordination is to be improved, were not mentioned.

REFERENCES

Federal Facilities Council (FFC). 2004. *Key Performance Indicators for Federal Facilities Portfolios.* Washington, D.C.: The National Academies Press.

General Accounting Office (GAO). 1998. *Leading Practices in Capital Decision-Making.* Washington, D.C.: GAO.

GAO. 2002. *Using Strategic Human Capital Management to Drive Transformational Change.* Washington, D.C.: GAO.

Office of Management and Budget (OMB). 2007. *Program Assessment: Bureau of Reclamation–Site Security.* Available at http://www.whitehouse.gov/omb/expectmore/summary/10003701.2005.html.

OMB. 2008a. *Program Assessment: FBI Intelligence.* Available at http://www.whitehouse.gov/omb/expectmore/summary/10003811.2006.html.

OMB. 2008b. *Program Assessment: National Park Service-Park Police.* Available at http://www.whitehouse.gov/omb/expectmore/summary/10003727.2006.html.

Office of Personnel Management (OPM). 2007. *Ensuring the Federal Government Has an Effective Civilian Workforce.* Available at http://www.opm.gov/ses/qualify.asp.

5

Conclusions and Recommendations

During the course of the study, the committee concluded that an effective security program that will lead to the development of a culture of security at Reclamation requires all of the following:

- A risk management approach.
- An integrated security plan for each facility.
- Policies and operational guidance for key aspects of the program.
- A collaborative operating environment.
- Senior management support and commitment.
- Adequate resources.
- Performance measurement and evaluation to support continuous improvement.
- A method for disseminating lessons learned.
- A vision and a long-term plan for a sustainable program.

CONCLUSIONS

Reclamation's security program has been driven by the urgency to provide some level of protection to a large number of facilities in the wake of the 1995 bombing of the Murrah Building in Oklahoma City and the 9/11 attacks on the World Trade Center and the Pentagon. In the committee's opinion, Reclamation has made significant progress toward establishing an effective security program. However, the committee's overall conclusion is that although the Bureau of Reclamation is now

better able to protect its infrastructure and its people against malicious acts than it was 7 years ago, the security program is not yet mature, well-integrated, or appropriately supported at all levels of the organization.

To date, Reclamation has focused on tactical issues: developing a risk management approach; establishing security plans for each facility; staffing a security and law enforcement office; and developing an intelligence gathering and analysis capability. Still missing are policies and operational guidance for effective responses to security-related incidents; performance measures to support continual improvement; and a method for disseminating lessons learned. Also missing are the full support and commitment of senior executives and managers at all levels of the organization and adequate resources—staff, expertise, and funding—to develop a security program that is robust and sustainable.

It is now time for Reclamation to take a more strategic approach to its security program. One of its highest priorities should be the development of a vision and a plan to provide a path forward. The vision should explicitly link the physical assurance of Reclamation's facilities to its overall mission of providing water and power. The plan should address policy, programmatic, and resource issues and should have the support and commitment of all of Reclamation's managers.

RECOMMENDATIONS

The committee's findings and recommendations follow. The recommendations are intentionally general to allow Reclamation and the SSLE Office some flexibility in determining what processes, tools, or policies will be used to address them. In some cases a recommendation relates to more than one finding.

With the exception of the development of a vision and a plan for the security program, the committee has not presented its recommendations in order of priority. However, some recommendations require action sooner than others because they will help to avoid undesirable outcomes and will yield both immediate and long-term benefits. These actions include the development of

- An out-of-cycle process for security assessments;
- Policy on the use of deadly force;
- Response plans for security-related incidents;
- A streamlined personal identity verification process;
- A pre-project planning process for security-related projects; and
- Policies related to the sharing of intelligence-based information.

A RISK MANAGEMENT APPROACH

Finding 1: The risk management process that Reclamation has developed to assign priority for conducting threat and vulnerability assessments, security improvements, and resource allocation is appropriate. Elements of this process, however, need to be continually improved and refined as threats emerge, as risk assessment methods evolve, and as research-based information becomes available.

Finding 2: Reclamation plans to conduct security assessments on a 3- to 6-year cycle even though security threats are continually emerging and must be continuously monitored.

Discussion of Findings 1 and 2

Reclamation has developed a risk management program that incorporates a screening procedure; threat scenarios; vulnerability and risk assessments for individual facilities; a cost-benefit analysis for risk mitigation measures; and a decision analysis framework. The grouping of Reclamation's facilities into categories that reflect relative risk and consequences (screening procedure) has been useful in assigning priority for mitigation projects and resource allocation. Different methods, including RAM-D, MSRA, and the Balanced Survivability Assessment Approach, have been used to conduct threat and vulnerability assessments; these methods are all accepted, standard, and appropriate. To remain abreast of the evolving field of risk assessment, BOR should monitor the new threat and risk assessment methods being developed by the Department of Homeland Security (DHS) and other organizations. In the future, Reclamation managers should be ready to use risk assessment methods recommended by the DHS and methodologies that are customized to the specific requirements of dam security, such as RAM-D.

Reclamation has patterned its risk management programs after its safety of dams program. Although there are differences in the types of threats being assessed, there are also opportunities to better integrate these programs. Staff have, in fact, indicated that SSLE is moving toward an all-hazards risk management approach that incorporates risks from natural hazards, malicious acts, accidents, and human error. An all-hazards approach would be consistent with the National Infrastructure Protection Plan. Currently, however, Reclamation's safety of dams program and its security program operate independently.

For the safety of dams program, Reclamation has institutionalized a rigorous review of every critical dam under its purview. Comprehensive facility reviews (CFRs) are performed every 6 years with participation of subject-matter experts from all levels of BOR. CFRs include a detailed site

examination, a review of changes in the state of the art, and an evaluation of risks. They look at many things, such as loading conditions on the dam and downstream populations. Periodic facility reviews (PFRs) are performed midway between CFRs and involve detailed site examination of the structures. Annual inspections are conducted by the area offices in years CFRs or PFRs are not held. The various reviews are designed to also identify important operational and maintenance needs.

In 1998 BOR established a "risk cadre" composed of five experts at the Technical Services Center to further the development of risk analysis processes for dam safety. The risk cadre developed a consistent risk analysis methodology, developed toolboxes for loading probability and consequences, and trained others in risk analysis with the objective of continually improving Reclamation's risk analysis processes. The expertise of this cadre could be expanded to include security-related issues, processes, and training to leverage resources and move toward an all-hazards approach.

By more fully integrating the dam safety program with the dam security program, Reclamation could create a synergy that would heighten awareness of security issues and, ultimately, reduce the overall risks to dams. If Reclamation were to use inspection teams whose members had both safety and security expertise, it might be able to better leverage its resources. For example, the NCI facilities now consume more than half of BOR's security funding. Dam safety resources and business processes, by contrast, are applied to a far larger set of dams. If dam security assessments were conducted together with all dam safety assessments, it might be possible to conduct a greater number of security assessments per cycle. In addition, the increased awareness of security issues among all the team members would benefit Reclamation in both the short and long terms. Training these teams to assess both safety and security risks would add to Reclamation's body of knowledge about the security of dams and provide for greater continuity in institutional knowledge as personnel change jobs or leave the organization. It is also possible that risk mitigation projects could be formulated that would address both safety and security vulnerabilities and result in multiple benefits for both the programs and the public.

Combining teams and resources in this way might cost more, at least initially. Also, care would need to be taken to ensure that dam safety does not suffer. For these reasons, it may be best to first try a combined approach on a limited basis to better understand the consequences, both positive and negative, before implementing it Reclamation-wide.

As noted in Chapter 3, security-related threats are continually evolving, so that a 3- to 6-year security assessment cycle similar to the dam safety inspection cycle might not be adequate in all cases. While the com-

mittee supports the implementation of a fixed cycle to ensure that assessments are in fact completed, it believes that Reclamation should provide for out-of-cycle security assessments when circumstances change and dictate that a security assessment is necessary.

Recommendation 1: Reclamation managers should monitor the new threat and risk assessment methods being developed by the Department of Homeland Security and others and use those methods that are most appropriate for dams and related infrastructure (Finding 1).

Recommendation 2: In addition to conducting security assessments on a 3- to 6-year cycle, Reclamation should institute a process and criteria for conducting out-of-cycle assessments as threats emerge and circumstances warrant (Finding 2).

AN INTEGRATED SECURITY PLAN FOR EACH FACILITY

Finding 3: A robust facility security plan provides for defense in depth through an integrated system made up of obstacles that restrict access, surveillance and intrusion detection systems, and a rapid-response force. Although elements of a facility security plan were visible at most sites that the committee visited, the elements did not appear to be effectively integrated.

Finding 4: At some sites, the committee could imagine threat scenarios, especially those involving insiders, that could not be countered effectively by the forces and fortifications in place. Too often facility security defenses appeared brittle and lacking in depth. If one line of facility security was neutralized, it was too likely that intruders could continue moving forward.

Finding 5: Reclamation evaluated a very limited number of standard threat scenarios for its security assessments. Security-related intelligence has not been integrated into site-specific, realistic threat scenarios to the committee's knowledge.

Discussion of Findings 3, 4, and 5

In the wake of the 9/11 attacks, Reclamation implemented a range of security improvements to protect its NCI dams and other critical facilities. The improvements include obstacles to restrict access, various types of surveillance and intrusion detection systems, and some response capabilities. It appears that for the most part the various measures were put in place as

individual components and were not well integrated to provide defense in depth. The committee also observed Reclamation's failure to integrate intelligence-based information into site-specific, realistic threat scenarios.

In the absence of realistic and specific threat scenarios, risk assessment programs may become bureaucratic exercises. The committee believes that effective training and contingency planning require consideration of a range of scenarios that are both site specific and responsive to current intelligence-based information. These scenarios should be tested in exercises that reflect the guidelines promulgated in FEMA's Homeland Security Exercise and Evaluation Program (HSEEP). Care should be taken to refrain from identifying any specific scenario as the anticipated mode of attack so long as other feasible options are open to an attacker.

Recommendation 3: Reclamation and the SSLE should review their facility security plans as a system, identify gaps in the integration of the various elements, develop a range of realistic, site-specific threat scenarios based on local conditions and intelligence from all available sources, and conduct both contingency planning and training exercises using these scenarios. A protocol for regular review and adjustment of scenarios should be adopted to assure that planning and training are aligned with current conditions (Findings 3, 4, 5).

Finding 6: Because each Reclamation facility is in a different jurisdiction with different laws and a unique mix of local, county, state, and federal law enforcement entities, the interface between first responders and those that provide follow-up will vary. Facility security plans will therefore need to incorporate distinct arrangements for cooperation among the various responders during a security-related incident.

Finding 7: Specific guidelines for command, control, and decision making at individual sites would enable an effective response to a security-related incident. At Reclamation, guidance for these responsibilities was unclear, and procedures were not well understood by staff.

Finding 8: Training exercises are important to ensure that when personnel from multiple government and law enforcement entities respond to a security-related incident, all of the key players understand the procedures for command and control and for the transfer of authority as events unfold. Training exercises need to be designed to test site-specific, realistic scenarios and to be aligned with the responsibilities of the responders.

Finding 9: Good communication is critical for an effective response to a security-related incident. The committee observed that some communica-

tion equipment and technologies used by Reclamation and other federal, state, and local law enforcement and security organizations were not interoperable and would hinder communication among responders.

Finding 10: Certain communication technologies used in rural areas are subject to failure caused by weather and related events and may not be reliable during a security-related incident.

Discussion of Findings 6 Through 10

In the event of a security breach or an actual attack on a BOR facility, a response by appropriately trained and equipped security or law enforcement personnel is called for. With few exceptions, such as the Hoover and Grand Coulee dams, Reclamation relies on local law enforcement entities to provide that response. Such entities typically have relatively little training in how to deal with security-related incidents.

Given constrained resources and the varying severity of risks to its facilities, Reclamation cannot (and probably should not) maintain an on-site response force for most of its facilities. Alternative security strategies must therefore be explored and implemented. For some of its most critical facilities, Reclamation should determine if the existing response force would be equipped and trained to respond to a significant security incident. For those facilities where an on-site force is justified by the potentially severe consequences of a dam failure or other event, Reclamation should determine if that force should be composed of Reclamation staff or the staff of an outside contractor. In other cases, Reclamation should consider if it would be beneficial to collaborate with local law enforcement to provide specialized security-related training for first responders. The security-related training given to Sacramento County law enforcement officials for response at Folsom Dam is an example.

The committee noted its concerns about differences in jurisdictional authorities, the dearth of command-and-control plans, unclear lines of communication, and the lack of interoperability of communications systems. These are issues that should be resolved in advance of a security incident through improved planning and training.

Better integration between the safety of dams program and the dam security program could result in some beneficial synergies among programs and staff, the leveraging of resources, and an overall improvement in security-related response capabilities. As part of the safety of dams program, Reclamation has developed emergency action plans for high and significant hazard facilities. These plans are updated annually. Tabletop and functional exercises are conducted regularly to practice responses to a simulated safety-related incident. These written plans

could be broadened to include responses to a security-related incident. The plans should clearly define the lines of authority, roles, and responsibilities of the security and law enforcement entities that would respond to a security-related incident. They should also describe the mechanisms and processes for ensuring operational coordination among all involved agencies and jurisdictions.

Testing of security-related responses would differ from testing dam safety in that there would not be any signs (such as seepage from a dam or torrential rains that could lead to an overtopping) warning that a dam failure is imminent. The procedures for notifying local officials and the public might need to be modified. Other changes might also be warranted.

Recommendation 4: Reclamation should ensure that all security and law enforcement entities that would respond to a security-related incident at one of its facilities have a clear understanding of the lines of authority, roles, and responsibilities outlined in the response plan. The various security and law enforcement entities at each facility should train together to practice the actions each entity would be responsible for in a realistic scenario (Findings 6, 7, 8).

Recommendation 5: Reclamation should ensure that its personnel have the appropriate equipment and skills to communicate with all other entities expected to respond to a security-related incident. It should validate the effectiveness of the communication methods through appropriate exercises and simulations and work to standardize communication approaches (Findings 9, 10).

Finding 11: The use of standard ammunition in some parts of some Reclamation facilities could substantially compromise the integrity of critical equipment. It was not clear if this was common knowledge throughout SSLE or among those security and law enforcement entities that would respond to a security-related incident.

Discussion of Finding 11

Discussions with selected SSLE personnel indicated that the use of standard ammunition in specific portions of facilities could substantially compromise the integrity of critical equipment. Spurred by this discussion, the committee also considered the role that nonlethal weapons and new technologies could play regarding forceful responses to malicious acts. A variety of weapons have been developed that can be used against suspected aggressors to impede or halt threatening actions. One such weapon is the Active Denial System, a microwave-emitting device that

heats the skin of those targeted by it. This weapon and others like it could be used to halt the advance of persons at the helm or wheel of a suspected mobile improvised explosive device before they pose a threat that would necessitate deadly force. Another new tool permits tactical teams to use noise-flash diversionary devices to break through doors by directing the energy from the devices at the locking mechanisms of doors. The committee believes that Reclamation would be wise to investigate such options as part of an overall review of its approach to dealing with potential terrorist attacks or other malicious acts.

Recommendation 6: Reclamation should investigate how nonlethal weapons and new technologies can be used effectively during a response to a security-related incident (Finding 11).

Finding 12: The committee observed design and installation flaws in several risk mitigation projects. The personnel at the relevant facilities clearly believed that such flaws could have been avoided if the SSLE staff had sought their input during the planning process, before the projects were designed and installed.

Discussion of Finding 12

Inadequate preproject planning has long been recognized as one of the variables that can most negatively affect a facility project (Smith and Tucker, 1983). A critical step in preproject planning is defining project scope and planning for execution because it is at this stage that risks are analyzed, preliminary designs are formulated, critical decisions are made, and the specific project execution approach is defined (FFC, 2003). Inadequate scope definition inevitably results in the need for changes, which in turn causes rework, increases project time and cost, lowers productivity, and undermines the morale of the workforce (O'Connor and Vickery, 1986).

Stakeholder identification and team alignment are also critical to project success. A typical preproject planning team is composed of a wide variety of functional groups with diverse priorities, requirements, and expectations, such as facilities managers and tenants, technical representatives, fire marshals, designers, and security specialists. Alignment incorporates all of the distinct viewpoints into a uniform set of project objectives that meets the organization's mission and business requirements.

Implementing an effective preproject planning process for Reclamation's risk-mitigation projects should overcome the types of design flaws observed, avoid rework, use available resources more effectively, and

improve working relationships. SSLE should ensure that the appropriate stakeholders for each project and each facility are represented on the preproject planning team.

Recommendation 7: Reclamation should establish an effective preproject planning process to improve the design of risk mitigation projects, avoid rework, use available resources more effectively, and improve working relationships. The SSLE should ensure that representatives from the area offices and facility operators are involved early in the process when decisions are made about project scope and implementation strategy (Finding 12).

POLICIES AND OPERATIONAL GUIDANCE FOR KEY ASPECTS OF THE PROGRAM

Finding 13: The distinction between law enforcement and security within Reclamation is not clear, and the resulting ambiguity has raised issues regarding the use of deadly force during a security-related incident.

Discussion of Finding 13

P.L. 107-69 gives Reclamation law enforcement authority but does not address issues related to security or antiterrorism. Reclamation has been trying to operate its security program within the confines of P.L. 107-69, which has created issues in regard to the use of deadly force. Specifically, federal law enforcement officers and other armed personnel do not have clear guidance on how to determine when deadly force may be appropriate in a security-related incident. Developing such guidance, however, requires more than a Reclamation-wide policy statement. Because of the many statutes and local jurisdictions, policies on the use of deadly force will need to be developed in collaboration with individual state and local law enforcement officials so that the guidance will be legally binding.

Recommendation 8: Reclamation and the SSLE should work with local law enforcement entities to expedite the development of clear, legally binding guidance on the use of deadly force. The guidance should clearly address how the defense-of-life rule might apply in specific types of security-related incidents (Finding 13).

Finding 14: Reclamation has not adequately addressed threats posed by insiders—Reclamation staff, facility operators, contractors—to override physical security components and take control of dam operations.

Discussion of Finding 14

The use of insiders by terrorists—through physical coercion or by collaboration—to override security components and seize operation of a facility is a serious threat. A single individual with knowledge of dam operations, such as a disgruntled employee, could also pose a serious threat. An insider could be a Reclamation or water and power authority employee or one of the many contractors who have access to some Reclamation facilities on a daily basis.

Although contractors are required to undergo the PIV process, it is not clear whether PIVs are used routinely and consistently across the five BOR regions.

Reclamation managers and personnel acknowledged the threat posed by insiders. However, the committee was not convinced that the threat had been fully appreciated or that effective measures to prevent or respond to such a threat had been fully developed.

Recommendation 9: Reclamation should determine if there are ways to streamline the personal identity verification process for employees and contractors while ensuring that the process remains effective in identifying those who may pose a threat to security. Criteria and a program for conducting periodic security reviews for key Reclamation personnel should also be developed (Finding 14).

Finding 15: Reclamation-wide guidance on site access procedures for contractors and on safeguarding plans and drawings for construction projects has not been issued. In the absence of such guidance, some area offices have developed their own procedures.

Discussion of Finding 15

With numerous ongoing construction projects, plans and drawings for Reclamation facilities and projects are used by staff and contractors daily. The *Reclamation Manual* does not include guidance on the safeguarding of plans or limitations on the number of copies in circulation.

The report *Managing Construction and Infrastructure in the 21st Century Bureau of Reclamation* said that "consistently implementing Reclamation's mission will require clear statements of policy and definitions of authority and standards (NRC, 2006, p. 97). It recommended that "policies, procedures, and standards should be developed centrally and implemented locally" (NRC, 2006, p. 98).

These statements also apply to Reclamation's security program. In some cases, such as personnel security clearances, Reclamation can adapt government-wide guidance (HSPD-12) to its specific situation. In other

cases, Reclamation may have to look to other federal agencies with similar programs. Where SSLE has drafted policy guidance and standards, that guidance should be vetted with the area and regional offices and modified as needed, so that approval can be sought from Reclamation's senior management as soon as possible. Policy guidance should always have some flexibility that allows for its adaptation to local situations.

Recommendation 10: Reclamation and the SSLE should move expeditiously to develop policies for site access for contractors and for the safeguarding of project plans and drawings. Policies should be formulated in close collaboration with area and regional managers and should be flexible enough to distinguish among different situations (Finding 15).

Finding 16: The objectives and operating procedures for law enforcement are different from those for security. The legislation giving Reclamation law enforcement authority does not address issues of antiterrorism or security, nor does it permit Reclamation to directly hire its own law enforcement personnel.

Discussion of Finding 16

The committee is not in a position to recommend specific changes to the authorizing legislation. However, several areas of Reclamation's security program should be reviewed to determine if the authorizing legislation needs to be changed.

Currently, it is not within Reclamation's authority or responsibility to warn the public directly or to evacuate them in the event of an impending dam failure. The premise is that if a dam is in danger of failing owing to torrential rains, a design flaw, or other safety-related cause, there will be sufficient time to notify local authorities and to evacuate people before downstream flooding occurs. This operating procedure does not take into account a dam failure caused by a malicious act in which there may be little or no advance warning of downstream flooding. The committee believes this is an area that should be reviewed to determine if the current procedures remain appropriate in a security-related incident or if legislative or other changes are needed.

The committee recommends that Reclamation should first work with local entities and others to develop legally binding policies on the use of deadly force. Reclamation should also identify security-related issues that arise through its inability to directly hire law enforcement personnel. If Reclamation identifies gaps in its authority that constrain an effective response to a security-related incident, it may be necessary to go to Con-

gress to request authorizing legislation that is a better fit with Reclamation's mission, its operations, and its culture.

Recommendation 11: Reclamation's senior executives and security managers should identify the gaps in their authority for creating an effective security program and, if necessary, seek authorizing legislation that will allow implementation of a more robust program (Finding 16).

A COLLABORATIVE OPERATING ENVIRONMENT

Finding 17: With its largely decentralized organizational structure and heavy reliance on partnerships and contractors, Reclamation is fundamentally dependent on collaboration within and among organizations to achieve its mission. Imposing a centralized security program on a culture that is accustomed to distributed program management and authority has resulted in tensions and ineffective working relationships between the SSLE staff in Denver and the staff of regional and area offices.

Finding 18: Sound working relationships are based on effective communications and trust. Managerial actions and the behavior of SSLE's Denver-based staff have in some cases created distrust among the regional and area office staff that is damaging to internal working relationships and that limits the effectiveness of the security program.

Discussion of Findings 17 and 18

The 2006 NRC report *Managing Construction and Infrastructure in the 21st Century Bureau of Reclamation* states as follows:

> A major factor in achieving the desired balance between decentralized and centralized authority and responsibility is the quality and quantity of communication—particularly face-to-face communication. A lot can be achieved if managers at the area, regional, and headquarters levels know and trust each other. This trust is the product of consistent and open lines of communication. Without good communication, suspicions will grow and the organization will not function well. . . . Reclamation . . . needs to plan and budget for frequent meetings to exchange ideas on management and technical issues. (NRC, 2006, p. 38)

This statement applies equally to Reclamation's security program, which is managed centrally but is highly dependent on the field offices to identify potential threats and to prevent, deter, and mitigate them. Tension between the SSLE and the field offices is, in part, a function of the organizational structure and the relative newness of the security program.

Until security is embedded into Reclamation's culture, the program will operate as a bolted-on function.

Communication and trust are also a function of managerial behavior. When SSLE staff bypass regional and area offices to talk directly with local law enforcement or Reclamation stakeholders, fail to seek input on risk mitigation projects from the area offices and facility operators, or so restrict the flow of security-related information that it affects the ability of the field personnel to do their jobs, they signal their lack of trust and respect. The outcome is resentment on the part of the field personnel and poor working relationships that hinder the effectiveness of the security program.

Recommendation 12: SSLE managers should recognize and respect the importance that regional and area staff attach to their working relationships with their operators, contractors, and local law enforcement personnel. SSLE should work through the regional directors and area office managers when developing risk-mitigation projects and other activities that require the input of local law enforcement personnel, operators, and other stakeholders. SSLE should also intensify its efforts to communicate the goals, methods, priorities, and budget constraints of the security program through face-to-face meetings with regional and area office managers. To be effective, communication should routinely be two way (Findings 17, 18).

Finding 19: An inflexible commitment to the need-to-know doctrine inhibits the sharing of intelligence-based information among SSLE staff in Denver, the regional special agents, and the area office personnel who might be in the best position to deter some threats and who would be the first responders to an incident.

Discussion on Finding 19

The rationale for restricting the dissemination of classified information is clear. However, much information on suspicious activities or incidents is not classified but "sensitive," a more ambiguous category. Reports on incidents or the activities of suspect individuals or representatives of suspect groups often are not passed on to managers of neighboring facilities because the material is deemed to be sensitive. This lack of communication and overly restrictive information sharing frustrates conscientious, responsible operating officials, who feel they are not being given information that would allow them to meet their security-related responsibilities effectively. The holding back of information by the LEA also undercuts the authority and credibility of the RSAs and makes it unnecessarily difficult

for them to build trust and good working relationships with Reclamation field personnel and local officials.

The committee recognizes that the LEA is constrained in exactly how much intelligence-based information may be transmitted and to whom. It is not clear, however, whether the LEA has conveyed to the field offices what those constraints might be. Two-way conversations with field personnel by means of conference calls or face-to-face meetings about the goals, methods, constraints, and priorities of the security program could begin to build trust and improve working relationships. Improved working relationships would improve the effectiveness of the security program and help to embed security into Reclamation's culture.

Recommendation 13: SSLE staff should endeavor to find ways to better inform senior managers and field personnel about potential threats to facilities based on security-related intelligence. They should also communicate the constraints under which they operate, especially the restrictions on dissemination of intelligence-based information (Finding 19).

Finding 20: Field personnel and others who have reported potentially valuable information about suspicious activities to the SSLE in Denver only rarely receive feedback on how or if the information was used. As a consequence, some field personnel view security-related communication as a one-way street and are reluctant to report on information about suspicious activities since their effort appears to have no effect.

Discussion of Finding 20

The committee repeatedly heard that operations personnel who have reported information of potential intelligence value to an RSA or the LEA seem only rarely to be told if the information was useful. Because they receive no feedback, some quietly admit that they no longer bother to report information about suspicious activities. This reluctance to report information because there is so rarely any feedback could result in the failure to recognize a threat to Reclamation facilities in time to take preventive actions.

Recommendation 14: When security-related information is collected at the local level and forwarded to the Denver office, the SSLE should provide feedback on the disposition of that information. It should at least acknowledge receipt of the information and encourage continued reporting of suspicious activities (Finding 20).

Finding 21: Although the SSLE's Denver-based staff may have the technical skills to carry out their job responsibilities, they have not in general displayed the communication, negotiation, and team-building skills needed for the sound working relationships that are critical to Reclamation.

Discussion of Finding 21

Immediately after the 9/11 attacks, as Reclamation was creating the SSLE, positions were primarily filled by transferring people, some of whom may not have had much security-related experience, from elsewhere in Reclamation and the DOI. In the years since, Reclamation has made an effort to recruit personnel with backgrounds in security and law enforcement and to upgrade the organization's overall security-related knowledge, skills, and abilities.

Because Reclamation relies on good working relationships with internal staff and outside partners for effective operations, SSLE staff in particular need good communication, negotiation, and team-building skills. Training in these skills for current staff could help to improve internal and external working relationships and the overall effectiveness of the security program. When recruiting new personnel, special emphasis should be given to these types of skills in job descriptions and during the interview process.

Recommendation 15: Reclamation should provide the SSLE staff with additional training in communication, negotiation, and team-building skills (Finding 21).

SENIOR MANAGEMENT SUPPORT AND COMMITMENT

Finding 22: Creating an effective security program and a culture of security requires the dedicated support and commitment of Reclamation's managers at all levels of the organization. Currently, such support and commitment are uneven. Some managers clearly understand the link between Reclamation's mission and security, and they are spearheading efforts to implement effective security procedures and programs. Others regard security as an unwelcome intrusion into other activities and resent the redirection of resources from other activities to security.

Finding 23: Building commitment and support for the security program is primarily the responsibility of Reclamation's senior executives—the commissioner, deputy commissioners, and regional directors and the director and program managers of the SSLE Office.

Discussion of Findings 22 and 23

To develop a culture of security, every employee, contractor, and stakeholder affiliated with Reclamation should be involved in security in some capacity. All employees and those contractors who work at BOR facilities should be aware of and educated about Reclamation's security policies and procedures. Contractors, operators, and other stakeholders, including suppliers (hydroelectric, irrigation, and water districts), should have an understanding of BOR security as it affects their roles and responsibilities.

Reclamation's commissioner, deputy commissioners, and regional directors and the SSLE director and program managers are responsible for leading change within the organization and leading people to achieve the organization's mission. Development of a security program and a culture of security represents a significant change within Reclamation. The link between security and achievement of Reclamation's mission must be consistently communicated from the top of the organization if security is to be fully supported at the field level. The dynamic nature of security-related threats must also be addressed to guard against complacency. Reclamation's facility operators, contractors, and stakeholders must understand that implementation of physical improvements and the hiring of site security guards is not the endgame but the beginning of a continuous process.

Recommendation 16: Reclamation's senior executives and SSLE personnel should clearly communicate the critical link between security and Reclamation's mission. Management must guard against sending the wrong signals to field personnel: that terrorism "can't happen here [in rural America]"; that field personnel and operators no longer need to be vigilant; or that threats no longer exist because some steps have been taken to improve the security of facilities (Findings 22, 23).

ADEQUATE RESOURCES

Finding 24: The resources—number of staff, expertise, funding—currently available for Reclamation's security program are not sufficient to operate and sustain an effective program.

Finding 25: Folsom Dam requires special consideration within the national critical infrastructure classification owing to the magnitude of the potential consequences of a security-related failure. The level of resources required for effective security is greater at Folsom than elsewhere.

Discussion of Findings 24 and 25

An effective security program must have enough people possessing the necessary competencies to carry out assigned tasks and must be adequately funded. Reclamation is attempting to protect 450 facilities distributed across 17 states with fewer than 50 full-time-equivalent positions, supplemented by service contractors who provide intelligence analysis and site security. The program has primarily been funded by redirecting resources from other programs, including safety of dams and facilities maintenance, to security.

Although a majority of the available resources has so far been focused on the NCI facilities, including Folsom Dam, additional resources may be needed for these facilities, especially Folsom, in the coming years. For its other critical facilities, Reclamation has a backlog of risk-mitigation projects that have not been implemented, partly owing to a shortage of resources for designing and installing them. In addition, only three full-scale exercises have been conducted, again owing to resource limitations. Additional training for SSLE staff in communication, negotiation, and other behavioral skills is required to develop the sound working relationships that are fundamental to Reclamation's activities.

Reclamation's overall budget has been decreasing at the same time as demands for funding facilities operations and maintenance and security requirements have been increasing. The committee is not in a position to recommend specific staff or budget increases, nor would it be appropriate to do so. However, in the committee's opinion, trying to implement a wide range of programs and meet increasing demands with decreasing resources will result in less effective programs and undesirable outcomes. The consequences of a security-related failure of a critical dam under Reclamation's stewardship and the associated costs would outweigh the costs incurred to prevent such a failure.

Recommendation 17: High-level attention should be given to determining how to provide additional resources to support a more robust security program without compromising other activities that are critical to Reclamation's mission (Findings 24, 25).

Finding 26: Security improvements benefit the public at large and are not limited to a specific set of stakeholders. Reclamation's proposal to make some security-related costs fully reimbursable creates tension with its stakeholders. The safety of dams program, in which reimbursable project costs are split between Reclamation and its stakeholders, may serve as a model for developing criteria, a process, and a cost-sharing percentage for reimbursing the costs of some security-related operations and maintenance activities.

Discussion of Finding 26

To supplement security-related funding and reduce pressures on other programs, Reclamation has sought to make some security-related activities, especially site security guards, fully reimbursable and thereby shift the funding responsibility to water and power authorities and other beneficiaries. According to the SSLE, Reclamation currently devotes between $20 million and $21 million to security guard costs.

This initiative has become contentious for Reclamation and its stakeholders. Although designating projects that benefit a specific set of stakeholders as reimbursable is a well-established and accepted procedure within Reclamation and with its stakeholders, security projects also benefit the general public. It is therefore not unreasonable for water and power authorities or other stakeholders to object to fully funding activities that also benefit others. Some stakeholders are reluctant to provide the necessary funding, while others may simply lack the funds. Others may not agree with BOR's risk assessments or the measures needed to correct security deficiencies. Some of this controversy might be eliminated if the same cost-sharing mechanism used for some operations and maintenance costs related to dam safety could be applied to dam security costs—that is, 85 percent federal funds and 15 percent stakeholder funds.

Recommendation 18: Where stakeholder reimbursements are sought for security-related operations and maintenance activities, the ratio that is used for the safety of dams program—85 percent federal funding and 15 percent stakeholder funding—should be considered as the starting point (Finding 26).

PERFORMANCE MEASUREMENT

Finding 27: Reclamation has developed some performance measures for evaluating the risk mitigation component of its site security program. Additional measures are needed to evaluate processes related to deterrence of and response to security-related incidents.

Discussion of Finding 27

Performance measures help organizations to identify where their objectives are not being met or where they are being exceeded. Managers can then investigate the reasons for this and make appropriate adjustments. Ultimately, an effective performance measurement system should inform decisions about the allocation of resources within an organization. Although it can be difficult to develop effective security-related perfor-

mance measures, some measures have been developed and are being used by Reclamation and other federal organizations.

Recommendation 19: Reclamation should establish a set of performance measures for its security program elements to encourage continual improvement. Where appropriate, it should use measures developed by other federal programs that are active in law enforcement and intelligence gathering. Performance outcomes should be measurable, achievable, and consistent (Finding 27).

A METHOD FOR DISSEMINATING LESSONS LEARNED

Finding 28: Lessons-learned processes can be useful for sharing experience-based information in an organization and for continually improving organizational processes, knowledge, and standards. Sources of lessons learned include after-action reports from training exercises, other forms of simulation, and other organizations.

Finding 29: Reclamation's security program does not appear to have a formal lessons-learned program in place. Where after-action reports followed major exercises, they were not disseminated to all the regions or the area offices that could have benefited from knowing the exercise results.

Discussion of Findings 28 and 29

A report of the Government Accountability Office stated that use of lessons learned is a key component of an organizational culture committed to continuous improvement (GAO, 2002). Lessons-learned mechanisms communicate acquired knowledge effectively and ensure that beneficial information is factored into planning, work processes, and activities. They are a powerful way to share good ideas for improving work processes, facility or equipment design, and operation, quality, safety, and cost-effectiveness.

The after-action reports produced for Reclamation's training exercises are one source of lessons learned. For future exercises, Reclamation should consider using the template for after-action reporting provided in the HSEEP.

Recommendation 20: In the short term, SSLE should distribute after-action reports to the appropriate staff at all area and regional offices to leverage the knowledge gained from training exercises. The field staff should ensure that the documents are kept secure. In the longer

term, Reclamation should develop a process and a database for capturing and disseminating lessons learned by looking to other organizations and agencies that have successful lessons-learned approaches (Findings 28, 29).

A VISION AND A LONG-TERM PLAN

Finding 30: Among their other objectives, organizational mission and vision statements, plans, and goals are meant to inspire and motivate employees and stakeholders. Typically, they are driven by an organization's senior executives and reflect their priorities and values. Infrastructure security does not appear explicitly in Reclamation's mission and vision statements, plans, or goals. The failure to mention it conveys the idea that infrastructure security does not have the support and commitment of senior management, nor has it been given priority.

Finding 31: Reclamation does not appear to have a plan for a security program that is robust, mature, and sustainable. When asked about their goals for the security program, senior managers focused on tactical issues. Strategic issues, such as how security is to be embedded in Reclamation's culture and how regional security coordination is to be improved, were not mentioned.

Discussion of Findings 30 and 31

Mission and vision statements, plans, and goals are all important because among other things they are meant to inspire and motivate employees and stakeholders. An organization's vision and its strategic goals typically are communicated from senior executives to managers and line staff. Security is not explicitly addressed in Reclamation's mission statement, its vision statement, its plan for implementing the vision, or its overarching goals. If security were a well-established program embedded in Reclamation's culture, the lack of an explicit reference to it might not be significant. However, because security is a relatively new program, the failure to mention it in the organization's key statements about its mission and goals signals that it is not a priority at Reclamation and conveys a lack of support for it and commitment to it on the part of senior management. In the short term, Reclamation should consider addressing security in its vision and strategic goals statements, by linking secure facilities to the achievement of its mission.

If Reclamation is to develop a security program that is mature, robust, and sustainable, one of its highest priorities should be to develop a long-range plan. The vision statement for the security program should

explicitly state what it is designed to accomplish in relation to Reclamation's mission. For example, it might emphasize the physical assurance of Reclamation's facilities in the face of security threats, predicated on a culture of preparedness. If Reclamation moves toward integrating the dam safety and security programs, physical assurance would be an objective of an all-hazards approach.

Once a vision statement for the security program has been formulated, additional strategic goals and objectives can be set to provide a framework for addressing policy, program, and resource issues and for creating a culture of security that is as strong as Reclamation's culture of safety.

Recommendation 21: Where appropriate, Reclamation's leadership should emphasize in its policy statements the link between security and the achievement of Reclamation's mission. A plan for sustaining an effective security program should be developed. Such a plan should include a vision, goals, and objectives, and strategies for accomplishing them (Findings 30 and 31).

REFERENCES

Federal Facilities Council (FFC). 2003. *Starting Smart: Key Practices for Developing Scopes of Work for Facility Projects.* Washington, D.C.: The National Academies Press.

Government Accountability Office (GAO). 2002. *Using Strategic Human Capital Management to Drive Transformational Change.* Washington, D.C.: GAO.

National Research Council (NRC). 2006. *Managing Construction and Infrastructure in the 21st Century Bureau of Reclamation.* Washington, D.C.: The National Academies Press.

O'Connor, J., and C. Vickroy. 1986. *Control of Construction Project Scope.* Source Document 6. Austin, Tex: Construction Industry Institute.

Smith, M., and R. Tucker. 1983. *An Assessment of the Potential Problems Occurring in the Engineering Phase of an Industrial Project.* Report to Texaco, Inc. Austin, Tex.: Analysis, Inc.

Appendixes

Appendix A

Biographies of Committee Members

John T. Christian, *Chair,* NAE, is one of the nation's leading geotechnical engineers and a consulting engineer. He spent much of his career at the Massachusetts Institute of Technology and at Stone & Webster Engineering Corporation, where he was a vice president before he left to go into private practice. Dr. Christian has published over 90 papers and three books in the geotechnical and earthquake engineering fields. He is currently a consulting engineer in Boston and Newton, Massachusetts. Dr. Christian has actively served as a fellow and former chair of the Engineering Accreditation Commission of the Accreditation Board for Engineering and Technology (ABET), the organization that oversees the accreditation of engineering programs at universities. He is also a former chair of the American Society of Civil Engineers (ASCE) Geotechnical Engineering Division and edited the Society's *Journal of Geotechnical and Geoenvironmental Engineering*. An honorary member of ASCE and of the Boston Society of Civil Engineers Section, ASCE, Dr. Christian is the distinguished recipient of several honors and awards. In 1996, he received ASCE's Thomas A. Middlebrook Award for a paper on the uses of reliability approaches in which he applied probabilistic concepts to geotechnical engineering. In 1999 he was elected to the National Academy of Engineering. He holds B.S., M.S., and Ph.D. degrees in civil engineering from MIT.

Bilal M. Ayyub is a professor in the Department of Civil and Environmental Engineering at the University of Maryland and director of the

Center for Technology and Systems Management. He is engaged in research on uncertainty modeling and analysis, systems modeling, decision analysis, homeland security, various defense and infrastructure systems, safety systems, and mathematical modeling using statistics, probability theory, fuzzy sets, and the theory of evidence. He is a fellow of the ASCE, the American Society of Mechanical Engineers (ASME), and the Society of Naval Architects and Marine Engineers (SNAME). Dr. Ayyub is a recipient of the American Society of Naval Engineers (ASNE) "Jimmie" Hamilton Award for the best paper in the *Naval Engineers Journal* in 1985, 1992, 2000, and 2002; an award for the outstanding research-oriented paper in the ASCE *Journal of Water Resources Planning and Management* in 1987; the ASCE Edmund Friedman Young Engineer Award for Professional Achievement, 1989; the North American Fuzzy Information Processing Society's K.S. Fu Award for Distinguished Service, 1995; the ASCE Walter L. Huber Research Prize, 1997; and several leadership and distinguished service awards. He is the founder and cochair of the International Symposia on Uncertainty Modeling and Analysis. Dr. Ayyub is the author or coauthor of about 450 publications, including many books and textbooks. Dr. Ayyub holds a B.S. in civil engineering from the University of Kuwait and an M.S. and a Ph.D. from the Georgia Institute of Technology.

George H. Baker III is a member of the faculty at James Madison University and is involved in consulting with industry and government in the areas of critical infrastructure assurance, high-power electromagnetics, and nuclear and directed-energy weapon effects. He is the former director (1996-1999) of the Defense Threat Reduction Agency's Springfield Research Facility, where he was involved in assessing, protecting, and targeting critical underground, infrastructure, and mobile systems. He was instrumental in organizing the initial Joint Chiefs of Staff force protection program and assessment teams. Much of his career was spent at the Defense Nuclear Agency directing RDT&E related to hardening systems to nuclear effects. He is the recipient of the Defense Nuclear Agency's Legacy and Technical Achievement awards. He is presently a member of the congressional EMP Commission staff and a member of the Executive Board of the National Defense Industrial Association's Homeland Security Division. He is a founding member of the Virginia Alliance for Secure Computing and Networking and of the Directed Energy Professional Society. He is past chair of the Nonproliferation and Arms Control Technology Working Group focus group on buried facilities, the Underground Site Infrastructure Applications Working Group, and the International Technical Cooperation Program EMP Group. He is an EMP fellow and senior member of the IEEE.

Dwight A. Beranek is vice president and operations manager at Michael Baker, Jr., Inc., where he is program executive for the Federal Emergency Management Agency map modernization project. Mr. Beranek recently retired from the U.S. Army Corps of Engineers (USACE), where he served for more than 35 years in a variety of management and leadership positions. Most recently, he was deputy director of military programs at USACE's headquarters in Washington, D.C. In that position, he provided senior executive direction and leadership for multi-billion-dollar-per-year military construction programs. Previously, he was the chief of engineering and construction serving as USACE's civilian chief engineer for civil works and military missions. Before that, he served as director of engineering for the Great Lakes and Ohio River Division, working extensively with military, state, and local officials to deliver military construction and water resources projects. Mr. Beranek served as a member of the Federal Highway Administration's Blue Ribbon Panel on Bridge and Tunnel Security and led the establishment of the Infrastructure Security Partnership, a network of more than 100 professional organizations dedicated to reducing the vulnerability of our nation's built environment to terrorism and natural threats. He is a member of the Society of American Military Engineers (SAME), the ASCE, the National Society of Professional Engineers, and the Accreditation Board for Engineering and Technology. He is the recipient of the President's Medal of SAME and the President's Medal of ASCE. He was also awarded the Presidential Rank Award for Meritorious Senior Executive for contributions in the federal government. Mr. Beranek holds a B.S. in engineering from Northwestern University and master's degrees in public administration from American University and in business administration from Boston University.

Mark M. Hankewycz is director of security services at The Protection Engineering Group, PC. He has 20 years of security experience with expertise in planning and implementing integrated electronic security systems consisting of automated electronic entry control, intrusion detection, and camera systems. He has comprehensive experience in security guard force management, antiterrorism/force protection, policy and procedure development, security needs assessments, risk analysis, and threat assessments, and command-and-control systems integration. Mr. Hankewycz has developed security master plans and emergency preparedness and disaster recovery plans. He is a member of the National Fire Protection Association and the American Society for Industrial Security. Mr. Hankewycz holds a B.S. in business management from the University of Phoenix.

Jeremy Isenberg, NAE, is recent past president and CEO of Weidlinger Associates, Inc., a structural and civil engineering and software develop-

ment firm. Dr. Isenberg is an expert in the computational modeling of dynamic response of structures, especially those exposed to blast loads. He initiated the conversion of computational mechanics technology at Weidlinger Associates from defense applications to civilian uses such as geological prospecting, design of ultrasound search units for medical imaging, and for optical inspection of submicron features on silicon wafers. He is active on several professional committees of ASCE and the American Concrete Institute and is recent past president of the Structural Engineering Institute of ASCE. He served as a member of the Federal Highway Administration's Blue Ribbon Panel on Bridge and Tunnel Security. He is the recipient of the ASCE Ernest Howard Award for contributions to computational mechanics applied to blast effects on structures; of the C. Martin Duke Award for contributions to lifeline earthquake engineering; and of the Tewksbury Award of ASCE/SEI. He is a registered civil or professional engineer in several states. He is a member of the National Academy of Engineering. Dr. Isenberg received a B.S. in civil engineering from Stanford University and a Ph.D. in structural engineering from Cambridge University, where he was a Fulbright scholar.

L. Michael Kaas retired as director of the Department of the Interior's Office of Managing Risk and Public Safety. In that position he was responsible for facilities management, health and safety, and law enforcement and security policy in the Office of the Secretary. His 28-year career at DOI also included positions at the U.S. Bureau of Mines as associate director for information and analysis, chief of the Division of Resource Evaluation, chief of the Division of Environmental Technology Research, chief of the Office of Regulatory Projects Coordination, chief of the Division of Mineral Information Systems, deputy director of minerals information and analysis, and planning officer. He is a recipient of DOI's Distinguished Service Award and its Meritorious Service Award. Mr. Kaas is a member and past director of the Society for Mining, Metallurgy, and Exploration of the American Institute of Mining, Metallurgical, and Petroleum Engineers and a recipient of the Herbert Hoover Award. He has authored many technical papers. Mr. Kaas is a registered professional engineer in Minnesota and holds a B.S. in mining engineering from the Pennsylvania State University and an M.S. in mineral engineering from the University of Minnesota.

David A. Klinger is associate professor of criminology and criminal justice at the University of Missouri, St. Louis. He previously held positions as assistant professor and associate professor of sociology at the University of Houston. Before pursuing his graduate degrees, he worked as a patrol officer for the Los Angeles and Redmond (Washington) police depart-

ments. He has held research positions at the Police Foundation in Washington, D.C.; the University of Washington, Seattle; the Washington State Attorney's Office; and the Seattle Police Department. In 1997, Dr. Klinger was the recipient of the American Society of Criminology's inaugural Ruth Caven Young Scholar Award for outstanding early career contributions to the discipline of criminology. Dr. Klinger's current research focuses on the organization and actions of the modern police. He has written more than 25 scholarly articles, book chapters, and encyclopedia entries on a variety of police-related issues. His book on officer-involved shootings, *Into the Kill Zone: A Cop's Eye View of Deadly Force*, was published by Jossey–Bass in 2004. Dr. Klinger holds a Ph.D. in sociology from the University of Washington.

Richard G. Little is director of the Keston Institute for Infrastructure at the University of Southern California (USC), where he conducts research and develops policy studies to inform the discussion of infrastructure issues critical to California and the nation. Prior to joining USC, he was director of the Board on Infrastructure and the Constructed Environment of the National Research Council (NRC), where he developed and directed a program of studies in building and infrastructure research. He has conducted numerous studies on life-cycle management and the financing of infrastructure, project management, and hazard preparedness and mitigation and has published extensively on risk management and decision making for physical security and critical infrastructure protection. Mr. Little has more than 35 years of experience in planning, management, and policy development relating to public facilities, including 15 years with local government. Mr. Little holds a B.S. in geology and an M.S. in urban-environmental studies from Rensselaer Polytechnic Institute.

John A. McCarthy is the president of Kamal Advisory Services, LLC, in Dubai. He was previously executive director and principal investigator of the Critical Infrastructure Protection (CIP) project at the George Mason University School of Law, where he also holds a faculty appointment as research professor of security studies. Prior to joining the CIP project, Mr. McCarthy was a director in KPMG's mid-Atlantic risk and advisory services practice, where he provided computer security, critical infrastructure, and business continuity management solutions to government clients. Prior to joining KPMG, Mr. McCarthy served as a member of the professional staff of the Critical Infrastructure Assurance Office, which supported the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism at the National Security Council. He assisted in the development of an integrated national infrastructure assurance strategy to address risks and threats to the nation's critical infrastructures.

He was a commissioned officer in the U.S. Coast Guard, where he served for more than 20 years in a wide variety of field command and senior staff positions. His military and civilian awards include the Legion of Merit, the Meritorious Service Medal (three awards), the Combat Action Ribbon, and the Vice President's National Partnership for Reinventing Government "Hammer" Award. He holds a B.A. degree in psychology from The Citadel Military College of South Carolina and an M.S. in information resource management from Syracuse University.

Charles I. McGinnis retired from the U.S. Army as a major general and was a former director of civil works for USACE; more recently he served in senior positions at the Construction Industry Institute in Austin, Texas. He has also served as a senior officer of Fru-Con Corporation and as the director of engineering and construction for the Panama Canal Company and later as vice president of the company and lieutenant governor of the Canal Zone. As director of civil works, he was responsible for a $3 billion per year planning, design, construction, operation, and maintenance program of water-resource-oriented public works on a nationwide basis. He is a fellow of SAME, a fellow and life member of ASCE, and a charter member of the National Academy of Construction. He is a recipient of the U.S. Army's Distinguished Service Medal. Mr. McGinnis is a registered professional engineer in Texas and Missouri and holds a master's degree in civil engineering from Texas A&M University.

Karlene H. Roberts is a professor at the Haas School of Business, University of California at Berkeley, and a research psychologist at the Institute for Business and Economics Research at Berkeley. Dr. Roberts has expertise in the design and management of organizations and systems of organizations in which errors can have catastrophic consequences. The results of her research have been applied to programs in numerous organizations, including the U.S. Navy and Coast Guard, the Federal Aviation's Air Traffic Control System, NASA, and the oil and gas, financial, and medical industries. Dr. Roberts has published on a wide variety of organizational risk management issues. She is a fellow in the American Psychological Association, the American Psychological Society, and the Academy of Management. She has served on several NRC committees, including the Human Factors Committee, the Committee on NASA's Bioastronautics Critical Path Roadmap, the Committee on Work Environment for Nurses and Patient Safety, and the Committee on Core Competencies for Federal Facilities Asset Management. She has a B.A. in psychology from Stanford University, a Ph.D. in psychology from the University of California, Berkeley, and an honorary Ph.D. in management science from the Université Paul Cézanne Aix-Marseille III.

Randy Rossman is a 20-year veteran of the Miami-Dade Police Department (MDPD). He holds the rank of sergeant and is currently assigned to the Homeland Security Bureau, which has the primary responsibility for gathering, analyzing, disseminating, and maintaining criminal intelligence and for homeland security initiatives for the MDPD and provides information to federal, state, and local law enforcement agencies. In addition, the HSB conducts security and vulnerability assessments and identifies the security needs of critical infrastructures and sites within Miami-Dade County that could be targeted by terrorists. Sgt. Rossman supervises detectives assigned to the Infrastructure and Protections Section, which includes Miami International Airport and the Port of Miami. His section recently completed a buffer zone protection plan for the Turkey Point nuclear power plant. Sgt. Rossman holds a B.S. in economics from Florida State University.

Craig D. Uchida is president of Justice & Security Strategies, a consulting firm that focuses on homeland security, criminal justice, and public health issues. He provides training and technical assistance, develops and implements research and evaluation plans, and assists in implementing change within local, state, and federal organizations. Dr. Uchida has more than 25 years of experience in criminal justice and has worked with more than 35 police agencies during his career. More recently, he has assisted agencies and organizations in homeland security issues. He assisted the Major Cities Chiefs Association with its terrorist alert policies, worked in Alaska on the continuity of operations/continuity of governance planning (COOP/COG), and documented the Los Angeles Police Department's efforts to establish Operation Archangel, a multiagency approach to critical infrastructure protection. In addition, he is an instructor in homeland security at the Naval Post-Graduate School. He previously served as assistant director for grants administration and as senior policy adviser, Office of Community Oriented Policing Services; as director, Office of Criminal Justice Research, National Institute of Justice (NIJ); and as director, Evaluation Division, NIJ, at the U.S. Department of Justice. He previously served as assistant professor, Institute of Criminal Justice and Criminology at the University of Maryland, College Park. Dr. Uchida holds a B.A. from the University of California at San Diego, an M.A. in American history from the State University of New York at Stony Brook, and an M.A. and a Ph.D. in criminal justice from the State University of New York at Albany.

Appendix B

Briefings to the Committee and Discussions

OPEN COMMITTEE MEETINGS

January 31-February 2, 2007

Welcome and Opening Comment
David Achterberg, P.E.—Director, Bureau of Reclamation, Security, Safety and Law Enforcement Office (SSLE)

SSLE Program Reviews
David Achterberg—SSLE Overview
- Review of policies, procedures, and budget and program management
- Discussion of current issues in SSLE and in regional and area offices

Don Taussig—Security Program
Vincent Parolisi—Law Enforcement Program
Kathy Norris—Emergency Management Program

May 2-4, 2007

Executive Overview-SSLE
Larry Parkinson—Deputy Assistant Secretary, Law Enforcement, Security, and Emergency Management, Department of Interior

Risk Assessment Overview
David Achterberg—Dam Safety Risk Assessment Methodology

David Hinchliff, Kim Duran, and Rusty Schuster—Security Risk Assessments Program
Don Taussig—Other Security Risk Components

September 19-20, 2007

Organizations Addressing Similar Security, Law Enforcement, and Emergency Management Issues
Col. James Braxton—U.S. Army Corps of Engineers
Enrique Matheu—Department of Homeland Security
Doug Bellomo—Federal Emergency Management Agency

Bureau of Reclamation Headquarters Perspective
Larry Todd—Deputy Commissioner, Bureau of Reclamation

COMMITTEE DISCUSSIONS AND SITE VISITS AT RECLAMATION REGIONS

The committee organized itself into two- or three-member teams, with one team assigned to visit each of the five regions comprising the Bureau of Reclamation. The visits took place between June 3 and August 5, 2007. They included meetings with staff at the regional and area offices to include those with security, law enforcement, and emergency management functions. Also included was the operations staff at specific dam sites. The meetings addressed questions (listed below) developed by the committee. However, the committee informed each site in advance that formal responses to the questions were not required. The purpose of the questions was to provide each region with a deeper understanding of the overall issues being addressed by the study effort. The committee also encouraged each region to approach its site visit discussions informally, emphasizing that formal PowerPoint presentations were not required. Nonetheless each region was given broad latitude in how it communicated information to the team.

Meetings were conducted with the following Reclamation offices:

Great Plains Area Office—Casper, Wyoming
Lower Colorado Regional Office—Boulder City, Nevada
Mid-Pacific Regional Headquarters and Construction Offices—Sacramento, California
Pacific Northwest Snake River Area Office—Boise, Idaho
Upper Colorado Regional Office—Salt Lake City, Utah

Site visits were conducted at the following locations:

Anderson Ranch Dam
Arrowrock Dam
Davis Dam
Deer Creek Dam
Flaming Gorge Dam
Folsom Dam
Fremont Canyon Power Plant
Glen Canyon Dam
Grand Coulee Dam
Hoover Dam
Jordanelle Dam
Keswick Dam
Parker Dam
Pathfinder Dam
Seminoe Dam and Power Plant
Shasta Dam

DISCUSSION QUESTIONS

Current Picture

From your point of view, what are the key security-related issues for BOR now and in the next 5-10 years? What challenges will SSLE, as presently organized and resourced, face in meeting these issues?

Approximately how many staff positions are devoted to security and law enforcement in your regional office? Your area offices? What functions are they responsible for?

What training programs are in place or being used? How are security and law enforcement integrated in the training? What improvements would you suggest?

Security

Is SSLE moving in the right direction, from the region's perspective?

How does SSLE's approach to managing security risks compare to how such activities have been implemented by the regions?

What does the on-site physical security look like for each SCADA system or component?

Is there a concern for the physical destruction of any SCADA component?

Are you satisfied with the security, authentication, deployment, and operation of existing SCADA networks?

Do the on-site infrastructures use specialized protocols and proprietary interfaces?

Do security/physical plant managers believe that the SCADA networks are secure because they are "air-gapped" (i.e., not connected to the Internet)? How are you trying to instill a security mind-set among your staff and stakeholders? What problems arise in an environment that historically has encouraged openness and stakeholder involvement?

What issues arise in communicating with constituent groups when sensitive information is involved?

Who is involved with security at the dam/facility?

Do you have security guards on contract? How many? What is their work schedule? What is their role?

Have you thought about terrorist acts, such as where and how they would occur?

Describe the nature of the threats as you envision them.

What will you do about the threats? Who has the authority/responsibility for dealing with threats?

Have you engaged in target hardening (barricades, surveillance cameras, checking identification regularly, use of technology)?

Do you have a continuity of operations plan (COOP) in case something does occur?

Law Enforcement

Given that SSLE does not have its own employees for law enforcement, how is this task accomplished at your site?

How do you work with local law enforcement?

Are any joint exercises conducted? If so, how is this coordinated and executed?

How do you address the collection of incident information that could serve as intelligence for further analysis/review?

Describe any data- or incident-sharing activities that you have in place with the local law enforcement agencies.

Emergency Management

How is planning for emergency exercise programs conducted? Describe your emergency notification system. Who provides emergency assistance for casualties?

Are there actions the BOR/SSLE can take in tandem with the regions to improve downstream consequences?

Are there ways that BOR could be more effective in working with the regions in today's emergency management environment?

Is the emergency management program appropriately staffed and funded?

Does SSLE have the right interfaces with the appropriate stakeholders?

Processes, Function, Expertise

What is the expertise profile of your staff? Do any expertise deficits exist? If such deficits do exist, how is that impacting your ability to meet your mission objectives?

How is threat/incident information made available to you? What are the sources of that information? How would you assess the availability of threat information? Who determines what actions should be taken? How do you communicate threats/necessary actions to local municipal officials/staff?

Working Relationships

How can SSLE communicate with constituent groups/stakeholders within your region without compromising sensitive information?

Describe the relationships with SSLE's Denver office, Washington office, and the Department of the Interior.

Which other law enforcement agencies do you interact with (e.g., Bureau of Land Management, National Park Service)? Describe how this interaction takes place.

Who are your key stakeholders? Describe how you communicate/work with these groups.

What is the role of local/state law enforcement (sheriff's office, state police, county police, or municipal police) in handling routine crime and disorder problems? That is, do they respond to calls for service at the dam/facility? Do they provide statistics, crime reports, and other information to you on a regular basis?

Does local law enforcement engage in preventive patrol activities around the facility? Or do they only appear when called upon?

Does the regional office have a contract or memorandum of understanding with local law enforcement at those facilities where a working relationship exists?

How would you characterize your relationship with local/state law enforcement? Is it cordial, friendly, and helpful? Or does there appear to be a strain in the relationship?

What is the role of local law enforcement with respect to terrorism or natural disasters? Do you have a formal, written plan for handling these types of concerns? If a terrorist act or natural disaster took place, do you have a strategy for dealing with it (an incident command system, policies, procedures, etc.)?

Do you work with the Joint Terrorism Task Force or other task forces? How often do they meet? Do you share information? Is the NCI recognized as a potential target?

Appendix C

Two Approaches to Risk Assessment for Dams

OCCURRENCE/VULNERABILITY/IMPORTANCE APPROACH

The risk assessment method described below is intended to identify in detail vulnerabilities of individual dams. In this step, components of the dam—intake towers, spillways, turbine generators—are considered, as are countermeasures to deter attack on and/or mitigate damage should an attack occur. Three factors are paramount in this risk assessment approach:

- *Occurrence (O)*, also referred to as the threat likelihood or threat rating (*T*), is the likelihood that terrorists will attack the dam under consideration. It includes target attractiveness, perceived level of security, access to the site, publicity accruing to the attacker, number of prior attempts to damage the dam, and other factors. It is in this factor that the risk assessment for terrorist hazard differs most from natural hazards, for unlike natural hazards such as earthquake and flood for which the history of independent events is well-documented, the history of terrorist events is brief. As a substitute for quantitative knowledge of recurrence intervals of earthquakes or floods, expressible in probabilistic terms, we must work with relative likelihood of occurrence. Input to this factor may come from intelligence sources.
- *Vulnerability (V)* indicates how much the facility or population would be damaged or destroyed based on the structural response to a terrorist act. It is the likely damage resulting from various

terrorist threats (weapon type and location) and measures expected damage, outcome of the event, expected casualties and loss of use. Input to this factor typically comes from engineering analysis and expertise.

- *Importance (I)*, also referred to as the consequences (*C*) or asset value (*A*), is a characteristic of the facility, and is the same for any hazard. It indicates consequences to the region or nation in the event a dam is destroyed or out of service. Input to this factor comes from the Bureau, from the water and power districts, and from public safety officials.

Following a well-established technology for natural hazards risk assessment, these factors are combined in the form of a triple product to calculate a quantitative risk index as follows:

$$\text{Risk} = O \times V \times I$$

This triple-product approach is described in *Recommendations for Bridge and Tunnel Security* (DOT, 2003), in *The National Infrastructure Protection Plan* (DHS, 2006),and in *Risk Analysis and Management for Critical Asset Protection (RAMCAP)* (ASME/DHS, 2005), using the *T, V, C* approach. It is also described in *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings* (FEMA, 2005), using the *T, V, A* nomenclature.

The following illustrates application of the risk formulation shown above. It is intended as a quantitative illustration only, with numerical factors to show how the method works. The values assumed in the example do not apply to any particular dam.

Figure C-1 illustrates a typical concrete gravity dam (Gravity Dam A) and its components. For each of the nine components, credible means of weapon delivery for attack are identified e.g., pedestrian, vehicleborne, and waterborne. The likelihood (*O*) of each threat occurring is assessed and quantified on a scale of 0 to 1 as a function of four variables: access to the dam component for the attack to be carried out; security at the dam component against the attack; attractiveness of the target for attack of this type; and ability of aggressor to carry out the attack against the dam component.

The vulnerability (*V*) of each of the nine components identified to each identified attack type is quantified on a scale of 0 to 1 as a function of three variables: expected damage to the dam component if the attack occurs; expected closure of the dam if the attack occurs; and expected casualties if the attack occurs. Finally, the importance (*I*) of the dam is quantified on a scale of 0 to 1 as a function of eight variables: exposed population;

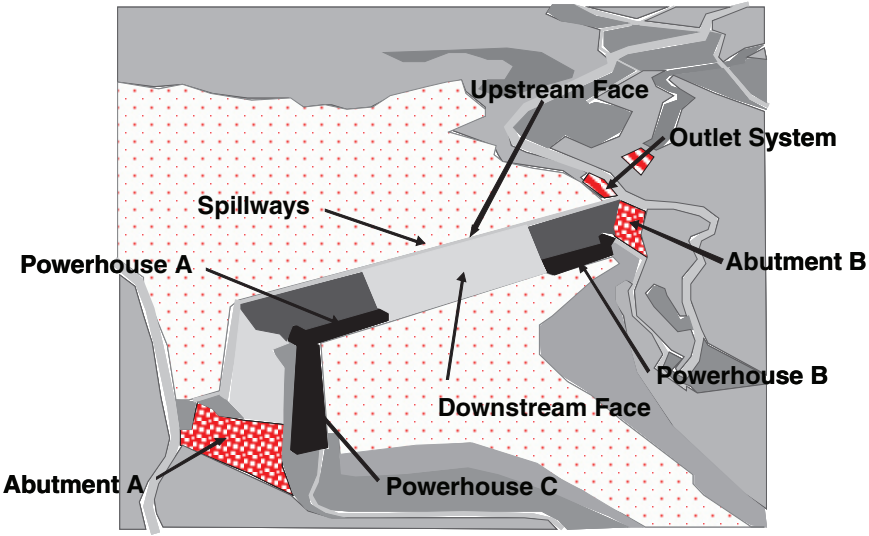


FIGURE C-1 Hypothetical concrete gravity dam (Gravity Dam A) and its components.

historical/symbolic importance; replacement value; importance to the regional economy; importance to the irrigation system; importance for power generation; importance to the transportation network; and annual revenue.

For each dam component-threat pair, the risk is quantified as the triple product of $O \times V \times I$. The risk to Gravity Dam A as a whole is quantified as the sum of the individual component-threat pair risk values. This is illustrated in Figure C-2, showing hypothetical values for Gravity Dam A and how they can be used to compare the risk for several dams assessed with the same process.

Quantifying risk in this manner allows for cost-benefit comparisons of alternative mitigation options. The benefit of each mitigation option is the reduction in the quantified risk for one or more dam component-threat pairs given the mitigation measures in place. For example, operational and electronic security measures reduce the likelihood of threat occurrence (O), while physical hardening reduces vulnerability (V), and changes in downstream exposed population can reduce or increase importance (I). Figure C-3 compares project costs and benefits for six mitigation alternatives at Gravity Dam A.

Threat Location	Transport	Risk = OxVxI
Abutment A	Water Borne	0.36
Abutment A	Pedestrian	0.65
Abutment A	Vehicle Borne	0.31
Abutment B	Water Borne	0.52
Abutment B	Pedestrian	0.71
Abutment B	Vehicle Borne	0.54
Powerhouse A	Pedestrian	0.72
Powerhouse A	Vehicle Borne	0.11
Powerhouse B	Pedestrian	0.68
Powerhouse B	Vehicle Borne	0.18
Powerhouse C	Pedestrian	0.88
Powerhouse C	Vehicle Borne	0.78
Upstream Face	Water Borne	0.85
Upstream Face	Pedestrian	0.82
Downstream Face	Pedestrian	0.89
Downstream Face	Vehicle Borne	0.92
Spillways	Pedestrian	0.29
Spillways	Water Borne	0.69
Outlet System	Water Borne	0.67
Outlet System	Pedestrian	0.09
Outlet System	Vehicle Borne	0.29
	SUM	11.95

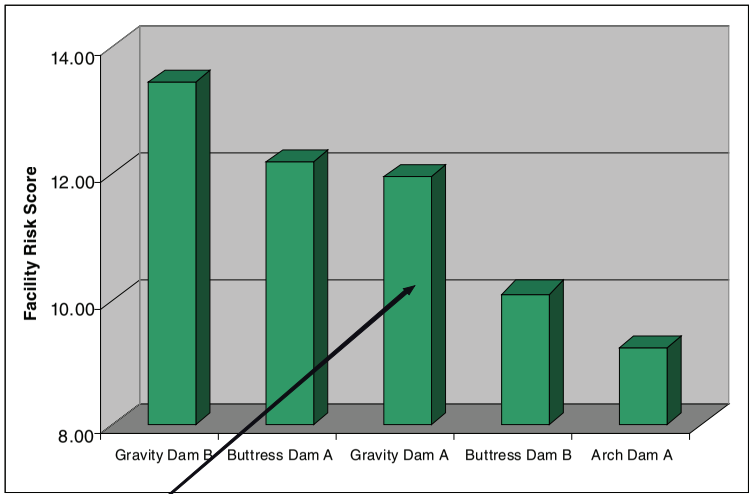
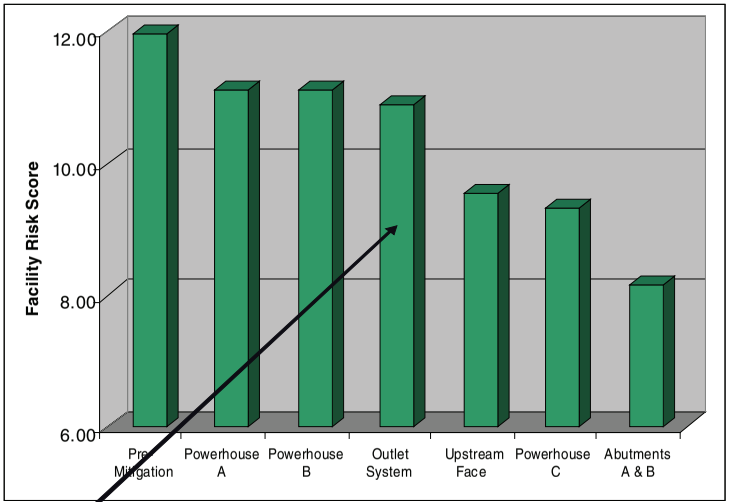


FIGURE C-2 Quantification of risk for the hypothetical Gravity Dam A compared with the risks for other hypothetical dams.



Mitigation Project	Cost ($1000)	Risk = OxVxI
Outlet System	750	10.88
Powerhouse A	2,840	11.09
Powerhouse B	2,840	11.09
Upstream Face	12,360	9.54
Powerhouse C	13,940	9.32
Abutments A & B	30,870	8.16

FIGURE C-3 Cost and benefit (reduction in risk) of six mitigation actions at hypothetical Gravity Dam A.

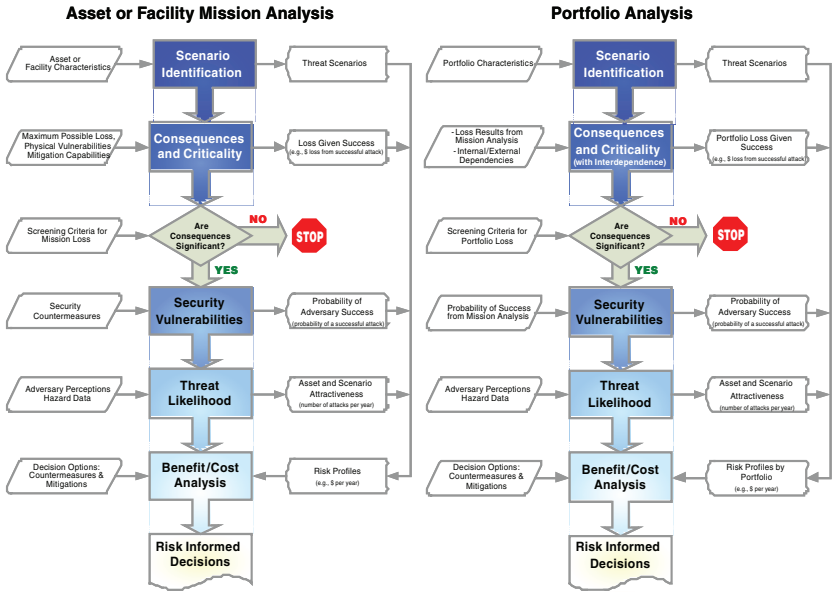
CRITICAL ASSET AND PORTFOLIO RISK ANALYSIS APPROACH

An alternative approach is the Critical Asset and Portfolio Risk Analysis (CAPRA) methodology, applied at the level of individual dams (Figure C-4). CAPRA was developed for the Department of Homeland Security and the Maryland Emergency Management Agency and has been used by the U.S. Army Corps of Engineers for the risk analysis of dams, office buildings, bridges, sports arenas, and regional protection. It is based on RAMCAP of ASME (2005) and is described by McGill et al. (2007) and Ayyub et al. (2007).

Similar to the OVI method, it surveys the dam's critical elements and couples them with knowledge of the consequences of disruption; physical and security vulnerabilities to a wide range of threats; and attractiveness, providing insight into actions an owner can take to reduce risk to a particular dam. CAPRA results are usually provided in the form of loss exceedance curves. The primary benefit of expressing results in this way is consistency with the way results obtained for natural hazards are currently expressed, enabling an all-hazards assessment.

According to the CAPRA methodology, risk is quantified and managed for critical infrastructure and key resource protection at two levels—the asset level and the portfolio level, including regional studies. An asset in this context is anything of value to its owner, such as a monument, vehicle, or facility.

- At the asset level, a survey of an asset's mission-critical elements coupled with knowledge of the consequences of disruption, physical and security vulnerabilities to a wide range of hazards and threats, and asset attractiveness provides insight into actions an asset owner can take to reduce an asset's overall risk exposure.
- The total risk associated with a portfolio or system of assets (such as those associated with a region, a jurisdiction, or an infrastructure sector) can be assessed in order to compare investment alternatives that aim to reduce overall portfolio risk. A portfolio in this sense is a collection of assets with common attributes or linkages. Regional analysis, for example, would define a portfolio top-down by first identifying the critical functions and services of the region and then assigning membership to regional assets that contribute directly to these mission areas. In contrast, a portfolio can be built bottom-up by first defining a set of assets, then examining how they relate to one another. In both the top-down and bottom-up cases, knowledge of the physical, geographic, cyber, and logical interdependencies among assets is important for assessing the potential for cascading consequences initiated by a hazard event.



(a) For an Asset (b) For a Portfolio and a Region

FIGURE C-4 Critical Asset and Portfolio Risk Analysis (CAPRA).
SOURCE: Ayyub et. al. (2007).

CAPRA is a phased process (Figure C-5) that systematically identifies hazard and threat scenarios that are relevant to the region or asset of interest; assesses the losses associated with each of these scenarios, allowing for consequence-based screening; assigns a probability of success; assesses the annual occurrence rate for each scenario; and provides results suitable for benefit-cost analysis.

CAPRA produces actionable risk assessments that inform a stakeholder of potential risks through custom-tailored risk communication reports and offers suggestions on what to do about them. These suggestions can help to identify alternative risk mitigation strategies and evaluate them for their cost-effectiveness, affordability, and ability to meet risk reduction objectives. The phases may be described as follows:

- *Scenario identification.* Characterizes the missions applicable to an asset, portfolio, or region and identifies hazard and threat scenarios that could cause significant regional losses should they occur. For natural hazards, this phase considers the estimated annual rate

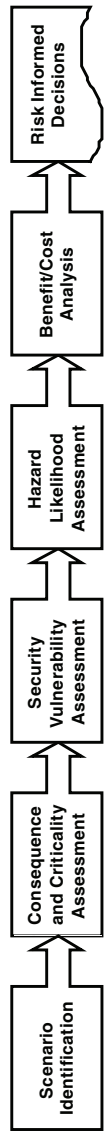


FIGURE C-5 Phases of the CAPRA process.

of occurrence and screens out infrequent scenarios. For security threats, this phase identifies relevant scenarios based on the inherent susceptibilities of a region's mission and lifeline services to a wide spectrum of threat types. The product of this phase is a complete set of hazard and threat scenarios relevant to the region under study.

- *Consequence and criticality*. Assesses the loss potential for each scenario identified for the region by considering the maximum credible loss, fragility of the target elements, effectiveness of mitigation strategies, and effectiveness of consequence-mitigation measures to respond to and recover from the loss. These assessments of potential loss are used to screen scenarios and identify those that warrant further analysis.
- *Security vulnerability*. Assesses the effectiveness of measures to deny, detect, delay, respond to, and defeat an adversary determined to cause harm to a region. This phase estimates the probability of an adversary's success for each threat scenario—which combined with loss—yields an estimate of conditional risk. This phase applies only to security threats; for natural hazards, the probability of adversary success is set to a default value of one.
- *Hazard likelihood*. Assesses scenario "attractiveness" from the adversary's point of view. The results from this phase provide estimates of the annual rate of occurrence for each threat scenario. For natural hazards, the results from this phase yield an annual rate of occurrence for a hazard affecting the asset.
- *Benefit-cost analysis*. Compares the cost of countermeasures and consequence mitigation with the benefit in terms of risk mitigation. The results of this analysis are used to inform resource allocation decisions.

REFERENCES

ASME/DHS (American Society of Mechanical Engineers/U.S. Department of Homeland Security). 2005. *Risk Analysis and Management for Critical Asset Protection (RAMCAP).* Washington, D.C.

Ayyub, B.M., W.L. McGill, and M. Kaminsky. 2007. Critical Asset and Portfolio Risk Analysis for Homeland Security: An All-Hazards Framework. International Journal of Risk Analysis. Vol. 27. No. 3. pp. 789-801.

DHS (U.S. Department of Homeland Security). 2006. National Infrastructure Protection Plan, Washington, D.C.

DOT (U.S. Department of Transportation).2003. Recommendations for Bridge and Tunnel Security. Blue Ribbon Panel on Bridge and Tunnel Security.

FEMA (Federal Emergency Management Agency). 2005. *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*. FEMA 452, Washington, D.C.

McGill, W.L., B.M. Ayyub, and M. Kaminsky.2007. A Quantitative Asset Level Risk Assessment and Management Framework for Critical Asset Protection. . International Journal of Risk Analysis. Vol. 27. No. 3.