DAMS SECTOR

Crisis Management Handbook

July 2021

Cybersecurity and Infrastructure Security Agency

Table of Contents

Agency Quick Reference Contact List

List incident reporting or response agency contact information for your community and geographic region. Build relationships with these groups before an incident occurs.

Resource	Contact	Phone Number
City Law Enforcement		
County Law Enforcement		
State Law Enforcement		
Local Fire Service		
Cybersecurity and Infrastructure Security Agency (CISA) Protective Security Advisor		
CISA Cybersecurity Advisor		
CISA Central	www.us-cert.gov/report Central@cisa.dhs.gov	(202) 282-9201
Local Joint Terrorism Task Force		
Local Federal Bureau of Investigation (FBI) Office		
FBI Weapons of Mass Destruction Coordinator		
FBI Hotline		1-800-CALL-FBI (800-225-5324)
State Dam Safety Office		
Downstream Dam Operator		
Upstream Dam Operator		
City Emergency Management		
County Emergency Management		
State Emergency Management		
U.S. Coast Guard		
State Fusion Center		
Information Sharing and Analysis Center (ISAC) (e.g., WaterISAC and Electricity ISAC)	www.waterisac.org/report-incident www.eisac.com/login	866-H20-ISAC (WaterISAC) (202) 790-6000 (E-ISAC)
Local Response Diving Unit		
Local Response Bomb Squad		

Acknowledgments

The Dams Sector Coordinating Council, Dams Sector Government Coordinating Council, Levee Sub-sector Sector Coordinating Council, Levee Sub-sector Government Coordinating Council, and the Cybersecurity and Infrastructure Security Agency (CISA), as the Dams Sector Risk Management Agency, acknowledge the active support from the public and private sector partners who contributed to the original development and subsequent update of this handbook.

The development of the 2021 update of the *Dams Sector Crisis Management Handbook* was led by the Dams Sector Security and Education Workgroup—comprised of members of the Dams Sector Coordinating Council, the Dams Sector Government Coordinating Council, the Levee Sub-sector Coordinating Council, and the Levee Sub-sector Government Coordinating Council—under the auspices of the Critical Infrastructure Partnership Advisory Council. The handbook was updated from the 2015 version to include guidance about additional planning document types and to reflect updates from primary source documents.

The cover photo, depicting The Dalles Dam in Oregon, is provided courtesy of the U.S. Department of Homeland Security (DHS).

Distribution

This document is available on CISA's Dams Sector Publications page at www.cisa.gov/dams-sector-publications and on the Homeland Security Information Network—Critical Infrastructure (HSIN-CI) Dams Sector Portal. The Dams Sector Portal within HSIN-CI allows for information sharing among federal, state, and local agencies and private sector owners and operators. For additional distribution information and access requirements for the HSIN-CI Dams Sector Portal, contact the Dams Sector Management Team at DamsSector@cisa.dhs.gov.

Notice

This material does not constitute a regulatory requirement; create any enforcement standard; or intend to conflict, replace, or supersede existing regulatory requirements. The statements in this document are intended solely as guidance. This document is not intended, nor can it be relied upon, to create any rights enforceable by any party in litigation.

The *Dams Sector Crisis Management Handbook* is one component of the Dams Sector Crisis Management Suite. Additional information is available at www.cisa.gov/dams-sector-publications, with all materials within the suite available on the HSIN-CI Dams Portal. Other associated handbooks, also available on the Dams Portal, that could be used by owners and operators to enhance their security posture include the following:

- **Dams Sector Security Awareness Handbook (FOUO):** An overview of how to recognize security concerns, coordinate proper response, and establish effective partnerships with local law enforcement and first responder communities.
- **Dams Sector Protective Measures Handbook (FOUO):** An overview of security strategies and protective measures addressing physical, cyber, and human elements and general recommendations for developing site security plans.

Introduction

Dams, levees, and related facilities are a vital part of the Nation's infrastructure, providing a wide range of economic, environmental, and social benefits through the delivery of critical water retention and control services. Dam projects are complex facilities that typically include water impoundment or control structures, reservoirs, spillways, outlet works, powerhouses, canals, and/or aqueducts. In some cases, navigation locks are also part of the project. While failures of these facilities do not happen often, dam failures are high consequence events. Security plans, emergency action plans, and dam safety programs are intended to reduce the chances of damage to these facilities and to limit the immediate consequences if failure does occur. Despite sound design, proper operation, and excellent emergency planning, a full or partial dam failure remains a real possibility. Therefore, an integrated crisis management approach can enhance the resilience of Dams Sector facilities by guiding emergency response and helping operators rapidly restore partial or full operations, while effectively communicating about the crisis and maintaining operations throughout the process.

More than 91,000 dams are listed in the National Inventory of Dams (NID), including dams over 25 feet in height or reservoirs with more than 50 acre-feet in storage capacity. In the NID, the downstream hazard potential (i.e., the amount of risk or damage a dam can pose due to failure or negligent operation) is classified as high, significant, or low. About 15,500 dams are classified as having a high-hazard potential.

Dams can fail for a number of reasons, including as a result of flooding, failure, error, or deliberate action. Certain characteristics of dams make them an unusually difficult type of facility to protect, particularly against deliberate attack. While critical assets in many other sectors are small or concentrated and can be contained within buildings, dams are often large facilities whose components are not necessarily enclosed within buildings. Dams are often located in remote areas and can be approached via land, water, or air. Some are required to provide public access to certain portions of the facility, which can create difficulty in controlling access around critical components.

Why Do Dams Fail?

- Overtopping caused by floods
- Structural failure
- Foundation failure
- Earthquake
- Piping and internal erosion
- Inadequate maintenance
- Operational errors
- Deliberate human-caused actions

Incidents involving Dams Sector assets could result in severe economic losses, loss of life, and reduced public confidence in industry and the government's ability to provide essential services. In the event of a dam failure, uncontrolled release of water stored behind even a small dam could potentially cause property damage and loss of life. Even if damage to a dam only prevents it from operating as intended, significant economic impacts could extend to the owner, the surrounding community, the region, and potentially the Nation.

The combination of benefits that our Nation derives from dams, the potential consequences of damage or disruption, and the difficulties in protecting dams can make them inviting targets for potential adversaries. Dam owners can reduce loss of life and property damage and enhance the overall resilience of their facilities through the development of a crisis management program inclusive of plans and exercises to guide emergency response, crisis communications, rapid restoration, and continuity of operations. An integrated crisis management approach enhances an organization's

ability to manage incidents that may impact the facility, disrupt operations, affect external stakeholders, degrade the ability to do business, or affect the brand and reputation of the organization. Each dam is unique because of differences in project configurations, engineering details, project benefits, and potential consequences from possible damage to the dam. Therefore, depending on the complexity of the facility and its operations, applying appropriate crisis management measures as part of a risk management program will be unique for each project.

About the Crisis Management Handbook

The *Dams Sector Crisis Management Handbook* explains how crisis management is an important component of an overall risk management approach and highlights basic elements of planning intended to minimize the consequences of damage or failure and return dam projects to full operations. Throughout the handbook, listed resources provide owners and operators additional information to continue to learn about and apply crisis management planning principles. This handbook is organized into the following chapters:

- **Crisis Management Programs:** Dam owners can enhance the overall resilience of their facilities through the development of a crisis management program inclusive of plans and exercises to guide emergency response, crisis communication, rapid restoration, and continuity of operations. This chapter defines the integrated crisis management approach and highlights several applicable standards and regulatory frameworks.
- **Understand Hazards:** Effective crisis management planning depends on understanding the threats and hazards the organization could encounter. This chapter introduces the threat and hazard identification and risk assessment process and highlights additional resources.
- **Develop Planning Documents:** The handbook includes a description of each of the following planning documents, including a definition, common elements of the plan, considerations when developing the plan, and resources to learn more:
  - **Emergency Action Plans:** The Emergency Action Plan (EAP) is a formal document that identifies potential emergency conditions at a dam and specifies actions to minimize loss of life and property damage. The EAP describes actions the dam owner/operator will take to moderate or alleviate a problem at the dam and to respond to incidents or emergencies related to the dam.
  - **Hazard-Specific Response Plans:** Several types of incidents—including cyber, active shooter, and explosives—escalate quickly and therefore require additional planning specific to the type of hazard. Hazard-specific response plans can effectively document the specific roles and responsibilities, requirements, and actions necessary to empower personnel to respond to a security incident without unnecessary delays.
  - **Crisis Communications Plans:** The initial phase of a crisis can be characterized by confusion, uncertainty, and intense media interest. Information is usually incomplete, and the facts often scattered. Crisis communications plans enable the organization to proactively establish effective and consistent communication with affected stakeholders by explaining how the organization will handle the crisis.
  - **Recovery Plans:** Damage to or failure of a dam can have long-term economic impacts to the dam owner, the community, other industries, or regional or national economies. Rapid restoration of dam functions can help minimize such impacts. Recovery plans address both short-term repairs to partially restore project functions and long-term repairs to fully restore the project.

  - **Continuity Plans:** It may be necessary to continue dam operations during the absence of several key personnel and/or primary operations locations. Continuity planning can identify personnel with the skills required to manage crises and to define shifts of roles and responsibilities to respond to the absence of key personnel.

- **Exercises:** While planning is essential for effective crisis management, periodic exercising of plans is necessary to test their adequacy and appropriateness. Exercises raise general awareness of potential crisis situations and ensure that key staff members are familiar with the plans and understand their roles and expected actions. This chapter outlines the benefits of conducting exercises, highlights common types of exercises and considerations when developing an exercise program, and resources to learn more.

The *Dams Sector Crisis Management Handbook* is one component of the Dams Sector Crisis Management Suite, which helps owners and operators understand the principles of crisis management and build a crisis management program. The suite includes educational materials, planning templates, and exercise support to test the plans included in the program. For additional information about the Crisis Management Suite, visit www.cisa.gov/dams-sector-resources. All materials included in the Crisis Management Suite can be accessed via the Homeland Security Information Network–Critical Infrastructure (HSIN-CI) Dams Portal. For access to the portal, contact the Dams Sector Management Team at DamsSector@cisa.dhs.gov.

Crisis Management Programs

Crisis management is the ability for an organization to manage incidents that have the potential to cause significant impacts. Critical to the success of crisis management is planning for an event, or series of events, that have the potential to severely impact operations, ability to do business, relationships with key stakeholders, brand, and/or reputation.

Crisis management is different from, although runs concurrent to, risk management, which focuses on identifying appropriate protective strategies and measures as part of a cost-effective plan to protect dams and prevent or minimize the potential for harm caused by both human-caused and natural disaster events. Any comprehensive risk management program must consider what happens if the dam is damaged, if dam failure is imminent, or if the dam has already failed—either partially or completely—regardless of the cause. Crisis management focuses on impacts to an organization's people, structures, systems, and operations. It is aimed at limiting consequences by containing the damage and preventing failure and minimizing the safety and economic impacts caused by damage or failure. For additional information on risk management, refer to the *Dams Sector Protective Measures Handbook (FOUO)*.

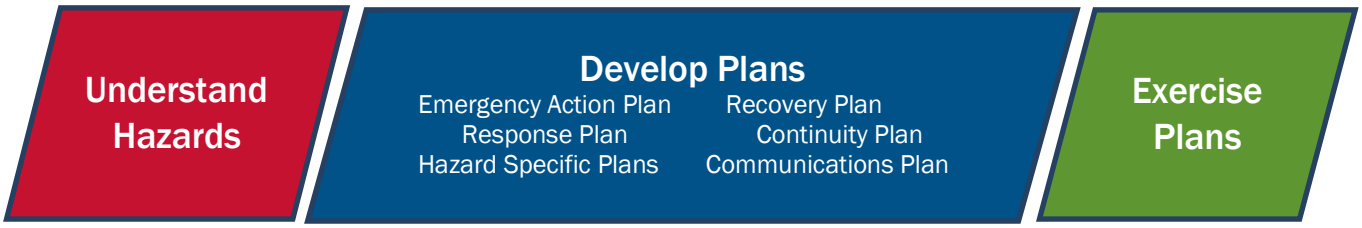
Owners, operators, and government agencies all have an important role to play in ensuring the safe and secure operation of dams and the reliable continuity of their benefits. A number of efforts can be pursued to enhance the safety, security, and resilience of these types of facilities while instilling public confidence in their operations. These efforts may range from actual physical modifications and cybersecurity measures to operational improvements and incident response planning activities. In particular, the increasing reliance on industrial control systems to direct physical processes and the use of connected technologies to remotely monitor operations heightens the importance of planning for incidents impacting both the physical and cyber domains.

Dam owners can enhance the overall resilience of their facilities through the development of plans to guide emergency response, crisis communication, rapid restoration, and continuity of operations. In general, these plans describe response actions that the facility will take for incidents and scenarios of concern. An integrated crisis management program inclusive of these plans serves as an overarching framework outlining how the facility will respond to an emergency or incident, regardless of the event or triggering source. Crisis management programs are intrinsically linked to the risk management strategies adopted by the organization as they focus on minimizing safety and economic impacts, limiting operational disruptions, and achieving prompt recovery.

As depicted in Figure 1, developing a crisis management program includes three components:

- **Understanding hazards** that could impact the facility, its operations, equipment, and personnel.
- **Developing plans** to prepare for, respond to, and recover from the likely hazards.
- **Conducting exercises** to validate and update plans, test communications protocols, and clarify roles and responsibilities.

Figure 1. Components of a crisis management program



A variety of standards and methodologies provide a comprehensive management systems approach to organizational resilience, preparedness, and business continuity widely applicable for private and non-profit organizations. The areas covered by these products are important elements of a crisis management program. Tailoring the lessons of the following standards and methodologies can address damage, disruption, or failure of Dams Sector facilities, and their resulting impacts on human safety and infrastructure. Links to access these products can be found in Appendix B. Bibliography.

- National Fire Protection Association (NFPA) 1600: Standard on Continuity, Emergency, and Crisis Management
- International Standards Organization 2301: Security and Resilience—Business Continuity Management Systems
- ASIS International, Organizational Resilience Management, ASIS ORM.1:2017: Security and Resilience in Organizations and their Supply Chains Standard
- Federal Emergency Management Agency (FEMA), Comprehensive Preparedness Guides (CPG)
  - CPG 101: Developing and Maintaining Emergency Operations Plans
  - CPG 201: Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review Guide, 3rd Edition
- MITRE: ATT&CK® for Industrial Control Systems

In addition to voluntarily complying with standards and methodologies, some organizations are required by regulation or statute to develop and exercise emergency or incident plans. The following list, while not all inclusive, outlines primary requirements within the Dams Sector pertaining to security-related planning. Non-regulated entities may consider reviewing the requirements and voluntarily implementing provisions relevant to their operations, as an industry best practice. Links to access these requirements can be found in Appendix B. Bibliography.

- State dam safety offices regulate the majority of dams in the Nation, with many issuing requirements for EAPs. Emergency Action Planning for State Regulated High-Hazard Potential Dams (FEMA 608) summarizes planning and response requirements for high-hazard dams. Owners and operators should contact their respective state dam safety office(s) for an updated list of requirements.
- America's Water Infrastructure Act, Section 2013 requires community drinking water systems serving more than 3,300 people to develop or update risk assessments and emergency response plans (ERPs). The law specifies the components that the risk assessments and ERPs must address and establishes deadlines by which water systems must certify their completion to the Environmental Protection Agency.

- Federal Energy Regulatory Commission (FERC) Division of Dam Safety and Inspections, FERC Security Program for Hydropower Projects (Revision 3A) provides guidance on security requirements—including vulnerability assessments and security plans—for specific security group categories of FERC licensees.
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standard, CIP-008-6: Cyber Security—Incident Reporting and Response Planning specifies incident response requirements for Responsible Entities to mitigate the risk to the reliable operation of the Bulk Electric System as the result of a cyber security incident.
- Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements establishes the framework, requirements, and processes to support the development of federal continuity programs, including specifying and defining elements of federal agency continuity plans.

Understand Hazards

Effective crisis management planning depends on understanding the threats and hazards that a particular organization faces. This is typically performed through a threat and hazard identification and risk assessment process that collects information about the natural hazards, technological hazards, and human-caused incidents that challenge the organization's ability to deliver its purpose or benefit. A sample list of such incidents related to the Dams Sector are listed in table 1.

Hazards may impact:

- Health and safety of persons in the affected area and those responding to the incident
- Continuity of operations
- Property, facilities, assets, and critical infrastructure
- Delivery of the organization's services
- Legislated, regulatory, and contractual obligations

Through this assessment process, the organization provides context to each threat or hazard by describing the risk and/or assigning values of risk for the purposes of deciding which threats and hazards the plan(s) should prioritize and subsequently address. Evaluating risk involves estimating the probability that the specific threat or hazard will occur and the likely impacts, including the severity, notification timing, and duration. Conducting a risk assessment will ensure organizations understand the threats they face, prioritize their actions, identify and compare options, and effectively allocate their resources.

Potential sources of threat and hazard information can include the following:

- Expert knowledge about past or potential future threats or hazards
- Existing assessments (e.g., security, risk, and vulnerability) conducted by the organization
- Records from previous incidents, including historical data
- Forecasts or models of future risks due to changing weather and demographic patterns
- Input from local law enforcement and/or emergency management agency
- Information and/or intelligence from a state or local fusion center
- National threat alerts and bulletins such as those issued by DHS and the Federal Bureau of Investigation (FBI), including the National Terrorism Advisory System, National Cyber Awareness System, or Technical Resource for Incident Prevention (TRIP*wire*)

The following resources are available to owners and operators to identify and prioritize threats and hazards on which crisis management planning efforts should focus:

- DHS, Dams Sector: Estimating Loss of Life for Dam Failure Scenarios
- FEMA, CPG 201: Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review Guide, 3rd Edition
- FERC, Dam Assessment Matrix for Security and Vulnerability Risk
- FERC, Potential Failure Mode Analysis (PFMA)
- FERC, Risk-Informed Decision Making Methodology
- Sandia National Laboratory, Risk Assessment Methodology for Dams
- U.S. Bureau of Reclamation, Consequence Estimating Methodology: Guidelines for Estimating Life Loss for Dam Safety Risk Analysis

Table 1. Potential Crisis Management Incidents

Attack	A hostile (cyber or physical) action aimed at disrupting or destroying operational capability and/or causing significant damage to a facility.
Breach or Failure	Any condition characterized by total or partial loss of the capability to impound water.
Controlled Breach	A planned (non-emergency) breach of an impounding structure, possibly carried out to remove a facility from service or to make major repairs.
Cybersecurity Incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.
Earthquake	A seismic event affecting operations and structural performance.
Emergency Action Plan Activation	Implementation of the emergency action plan in part or whole.
Emergency Condition	Any event or circumstance that clearly compromises the structural integrity of a facility and could lead to breach or failure.
Equipment Malfunction	Failure of mechanical or electrical equipment to perform the functions for which they were intended.
Excessive Release	Reservoir discharge that exceeds downstream capacity and/or causes downstream damage.
Facility Mis-Operation	Unintentional operator error affecting the operations of a facility.
Lock Closure	Unscheduled or scheduled interruption of partial or total navigation traffic through a facility.
Physical Security Incident	Any breach in access control systems such as fences, doors, gates, locks, and security zones.
Regulatory Action	The regulatory agency has determined that an unsafe condition exists, or the facility does not meet applicable design criteria and requires action to be taken by the owner.
Reservoir Incident	Any event in a reservoir that may impact the structural/functional integrity of a facility.
Sabotage	A deliberate action aimed at weakening or destroying operational capability through subversion, obstruction, disruption, and/or destruction.
Security Posture Modification	Any change of security activities and protocols in response to specific threat reports.
Significant Inflow Flood	Operations and structural performance are affected by significant inflow flood.
Significant Inflow of Ice and Debris	Operations and structural performance are affected by significant inflow of ice and debris.
Structural Modification	Modifications to improve the safety and/or operational characteristics of a facility.
Suspicious Activity	Any indication that surveillance or other attack planning activities could be taking place.
Unsafe Condition	Any developing or occurring event or circumstance that may adversely affect the structural integrity of a facility but is considered controllable through the appropriate remedial actions.
Unsatisfactory Condition Report	The findings of any inspection, assessment, or investigation that identify unsatisfactory or unsafe conditions at a facility.
Unusual Observation	An unusual situation is detected, but there is no indication that the structural/functional integrity of a facility may be immediately compromised.
Vandalism/Theft	The willful or malicious destruction/defacement of public or private property, or the removal of personal property with the intent to deprive the rightful owner of it.
Vessel Allision, Collision, or Grounding	Any event involving vessel impacts on other vessels, structures, or operating equipment at a facility.

Emergency Action Plans

Emergency Action Plans (EAPs) are pre-disaster guidance documents that help dam owners and operators mitigate impending incidents due to breach or malfunction of their facility. An EAP provides pre-determined response protocols for various hazard scenarios addressing what could go wrong, how it would happen, who and what would be in danger, and how emergency personnel would respond and in what timeframe. By providing such protocols, EAPs can reduce property damage, loss of life, and further infrastructure damage by enabling quicker, more effective emergency responses. Therefore, an EAP also can dramatically reduce liability to the dam owner.

The dam owner is responsible for developing and implementing the EAP and ensuring it conforms to federal and state requirements. Development of the plan should be completed in coordination with state and local emergency management authorities to facilitate the implementation of the authority's emergency operations plans or warning and evacuation plans.

Central to an EAP are notification lists, which help expedite the mobilization of resources and communicate hazard warnings to local authorities, upstream and downstream dam owners, and the general public. EAPs also address a variety of preparedness issues, such as alternative communications systems, off-hour responses, emergency supplies, and equipment caches. The inclusion of inundation maps and other visual aids assist dam owners and emergency personnel to develop and implement effective response plans to potential disasters.

Every dam has unique geology, geography, vulnerabilities and populations at risk, and therefore requires an EAP specific to the dam. Resources and templates are readily available to help dam owners develop effective, site-specific EAPs. Once an EAP is on file, frequent trainings and exercises are important to maintain readiness and keep EAPs up to date.

Elements of an Emergency Action Plan

Notification Flowcharts and Contact Information. A notification flowchart supports the timely notification of those responsible for taking emergency actions by identifying who is to be notified of a dam safety incident, by whom, and in what order. As such, the flowchart must be tailored to the needs and priorities of each dam. Multiple charts may be necessary, depending on the complexity of the hazards associated with the dam and the potentially affected downstream areas. For ease of use during an incident, the notification flowchart(s) should clearly present the following information:

- Emergency level of the notification flowchart if more than one flowchart is required. For example, Level 3 (unusual event), Level 2 (potential failure), and Level 1 (failure imminent).
- Prioritization of notifications based on the specific hazards posed by the emergency. Some individuals may have more time-sensitive tasks, and therefore should be notified first. The flowchart should clearly detail this notification hierarchy.
- Individuals who will notify dam owner representatives and/or emergency management authorities, as listed below in table 2. It is usually recommended that one person be responsible for contacting no more than three or four other parties. The flowchart should list contact information for the individuals to be notified. Include primary contact information (e.g., names, positions, telephone numbers, and radio call numbers) and supplemental contact information (e.g., fax numbers, email addresses, direct connect numbers, and alternate contacts).

Table 2. Notification flowchart

Dam owners will contact:	Local emergency management authorities will contact:
• Engineer/management staff/public affairs officer • Local emergency authorities or 9-1-1 centers • State dam safety program representatives • Other regulatory authorities • Upstream and downstream dam owners	• Other local responders such as police or fire • State emergency management authorities • Affected residents and businesses • Appropriate National Weather Service Forecasting Offices

EAP Response Process. The following four steps make up the general EAP response process and should be discussed in the plan:

Step 1: Incident detection, evaluation, and emergency level determination

Step 2: Notification and communication

Step 3: Emergency actions

Step 4: Termination and follow-up

Within this general process, it is important to provide site-specific procedures for successful implementation of the EAP. Early detection and evaluation of the condition(s) or triggering event(s) initiates an emergency response action. Procedures for the reliable and timely determination of an emergency level facilitates appropriate response actions (e.g., preventive or mitigating procedures tailored to various conditions at the dam) and implementation of notification procedures. Procedures for early notification allow all entities involved with plan implementation as much time as possible to appropriately respond. Finally, procedures determine when termination of the incident is appropriate and what follow-up activities may be required.

Responsibilities. The EAP must clearly specify the responsibilities of entities involved in responding to an incident and implementing the plan to ensure that effective and timely action is taken when an emergency at the dam occurs. Dam owners are responsible for developing and maintaining the EAP and, in coordination with emergency management authorities, are responsible for implementing the EAP. Emergency management authorities with statutory obligations are responsible for warning and evacuation within affected areas. All entities involved with EAP implementation are responsible for documenting incident-related events.

Preparedness Activities. Preparedness, as it relates to an EAP for a dam, typically consists of activities and actions taken before an incident occurs. Preparedness activities attempt to facilitate incident response as well as prevent, moderate, or alleviate the potential effects of the incident. At a minimum, the EAP should address the categories related to preparedness listed in the text box to the right.

Preparedness Categories

- Surveillance and monitoring
- Warning sirens
- Evaluation of detection and response timing
- Access to the site
- Response during periods of darkness
- Response during weekends and holidays
- Response during periods of adverse weather
- Alternative sources of power
- Emergency supplies and information
- Training and exercising
- Alternative systems of communication
- Public awareness and communication

Inundation Maps. The primary purpose of an inundation map is to show the areas that would be flooded and travel times for wave front and flood peaks at critical locations if a dam failure occurs or there are operational releases during flooding conditions. Inundation maps are a necessary component of the EAP and are used by both the dam owner and emergency management authorities to facilitate timely notification and evacuation of areas potentially affected by a dam failure or flood condition.

Appendices. The appendices in an EAP should contain supplementary materials that would be useful to emergency management personnel in effectively implementing an EAP. These materials typically include primary documentation used to develop the EAP and information to assist with decision making during an incident, such as the topics listed in the text box to the right.

Examples of EAP Appendices

- Detailed operation and maintenance requirements
- Dam breach information and analyses
- Record of plan reviews and updates
- Plan distribution list
- As-built drawings
- Incident tracking forms

Considerations when Developing an Emergency Action Plan

Coordination with Emergency Planning

It is vital that the development of the EAP be coordinated with all entities, jurisdictions, and agencies that would be affected by an incident at the dam or that have statutory responsibilities for warning, evacuation, and post-incident actions. The EAP should contain clearly defined roles and responsibilities for each entity. Coordination with emergency management authorities responsible for warning and evacuating the public is essential for ensuring agreement on individual and group responsibilities. Involving all entities with responsibilities listed in the EAP in the development of the plan will enhance confidence in the EAP and its accuracy. This coordination will provide opportunities to discuss critical emergency planning concerns, such as the order of public official notification; use of backup personnel; alternate means of communication; and special procedures for use during nighttime, holidays, and weekends.

Communications Protocols and Systems

Reliable communications protocols and systems are essential during emergency situations to quickly exchange critical information between key individuals and organizations. The possibility of unreliable primary communications systems in times of emergency should be addressed during EAP development, as it may be necessary to have backup communications systems. These may include, but are not limited to, emergency sirens, cellular phones, direct connect, email, intranet, radios, social media, and couriers. Operating procedures and special instructions for using primary and backup systems should be described in the EAP and regularly tested prior to an emergency.

It may be necessary for the dam owner to assist emergency management authorities in developing public awareness measures. These measures typically explain the proximity of the dam, how people will be informed of an emergency, and the actions people should take during an emergency. The EAP should include a brief description of any planned public awareness measures. Emergency management authorities may consider the use of social media for both primary and alternate systems of communication with the public. Consider the target audience involved and the best means for communicating with them. For example, notification to residences, recreation areas, and campgrounds downstream from a dam can be challenging, as these populations require quick and effective communication to facilitate evacuation.

Evacuation Planning

An EAP should lay out who is responsible for evacuation of the dam facility itself. However, state and local emergency management authorities are responsible for downstream community evacuation planning and implementation. Although an EAP does not need to include a community evacuation plan, it should indicate who is responsible for coordinating with emergency management authorities for community evacuation.

Inundation maps developed by the dam owner must be shared with emergency management authorities and included in the EAP to help in the development of warning and evacuation plans. Dam owners should also include procedures in the EAP for ensuring that emergency management authorities are provided with timely and accurate information on dam conditions during an incident. This information will help agencies make the appropriate decisions on evacuations.

Coordination with Security Provisions

A security plan, if developed by the facility, should be coordinated with the EAP to align areas of potential overlap, reduce redundancy, and eliminate inconsistencies. To accomplish these goals, dam owners should include an appropriate security representative in the EAP development process. Other security-related provisions to consider when implementing an EAP include:

Security Plans

This handbook uses the term security plan when referring to a plan for a specific dam project. Various organizations within the Dams Sector might use the terms "site security plan" or "site-specific security plan" to refer to such a document and may instead use the term "security plan" to refer to an overall organizational plan. For more information about security plans, see the *Dams Sector Protective Measures Handbook (FOUO).*

- **Site Security:** If a dam safety incident is caused by a security incident, the dam site might remain dangerous if adversaries remain in the area with the intention of harming incident responders. Such intentions have been demonstrated at previous bombing locations within and outside of the United States. Any emergency situation (even if not caused by an attack) could be an especially sensitive time and the EAP should address necessary site security actions during these situations.
- **Cyberattack:** Dam safety incidents caused by cyberattacks should be considered during development of the EAP. During such an attack, an adversary targets the cyber system(s) to improperly operate the dam in order to cause damage.
- **Investigations:** If a security incident results in damage to a dam or dam failure, law enforcement agencies will be responsible for investigating the incident to identify and apprehend the perpetrators. This could complicate the incident command authorities among local responders and potentially interfere with emergency actions planned by the dam owner.

Declaring and Terminating the Emergency

The dam owner is responsible for making decisions that an emergency condition exists or no longer exists at the dam or that the level of the emergency has changed. The EAP should clearly designate the individual responsible for making those decisions if the dam owner is unwilling or unable to make this assessment. State or local emergency management officials will initiate and terminate evacuation or disaster response activities, in accordance with the National Incident Management System (NIMS). The dam owner and state and local officials should agree on when it is appropriate to terminate an emergency.

Post-Emergency Evaluation

Post-emergency improvement planning enables organizations to identify strengths and areas for improvement and take the corrective actions necessary to improve plans, build and sustain capabilities, and maintain readiness. Following an emergency, all participants should take part in a review that identifies and documents the following:

- Events occurring before, during, and following the emergency
- Significant actions taken by each participant and possible improvements for future emergencies
- Strengths and deficiencies found in procedures, materials, equipment, staffing levels, and leadership

Maintaining the EAP

After the EAP has been developed, approved, and distributed, continual reviews and updates must be performed to ensure the EAP does not become outdated and ineffective. The EAP should be reviewed at least annually for adequacy and updated as necessary to address changes in personnel and contact information, to the facility, or to emergency procedures. Regulated entities should review applicable requirements for updated EAPs, as some regulatory agencies require periodic updates at specific intervals. The review should include an evaluation of any modifications to the reservoir, downstream development, or changes in expected inundation areas. The review should also include a determination of whether any revisions, including updates to inundation maps, are necessary. Regardless of the need to revise the EAP, document the review date and scope on the plan.

An out-of-cycle review of the EAP may be prompted by the completion of an exercise, changes to the dam and/or inundation zone, or associated periodic review and verifications of personnel and contact information. Document modifications to the EAP associated with these prompts, such as updated emergency procedures, inundation maps, notification flowcharts, or contact lists.

Sensitive Information

Because EAPs often receive wide distribution, it may be necessary to exclude sensitive information from some copies. However, sensitive information could be included in the EAP as a supplement or as another appendix. Distribution of this portion could be limited to those individuals or agencies with a specific need-to-know.

Resources for Developing an Emergency Action Plan

The Dams Sector Crisis Management Suite includes templates to aid in the development of crisis management plans, including EAPs. All templates can be accessed on the Homeland Security Information Network—Critical Infrastructure (HSIN-CI) Dams Portal at hsin.dhs.gov/ci/ds.

The FEMA National Dam Safety Program (NDSP) offers publications to assist dam owners in improving dam safety. All NDSP resources can be accessed at www.fema.gov/emergency-managers/risk-management/dam-safety. The following documents pertain, in whole or in part, to emergency action planning:

- *FEMA P-93: Federal Guidelines for Dam Safety*, published in collaboration with the Interagency Committee on Dam Safety, aligns federal dam safety protocols (including guidelines for drafting EAPs) with the NDSP.

- *FEMA P-64: Guidelines for Dams Safety: Emergency Action Planning for Dams* expands upon the guidelines issued in FEMA P-93.
- *FEMA P-946: Federal Guidelines for Inundation Mapping of Flood Risks Associated with Dam Incidents and Failures* is intended as an adjunct to FEMA P-64 and can aid in the development of inundation maps for an EAP.

Federal agencies with dams under their purview have issued policy or guidance related to content and format of EAPs. For dams not under purview of these agencies, the policy or guidance listed on the following websites can be used as industry best practices in developing an EAP:

- The U.S. Department of Agriculture, Natural Resource Conservation Service EAP policy and sample EAP can be accessed at www.nrcs.usda.gov/wps/portal/nrcs/main/national/ndcsmc/.
- The FERC EAP Program guidelines can be accessed at www.ferc.gov/emergency-action-plan-eap-program.

State Dam Safety Offices—in every state except Alabama—regulate the majority of dams across the Nation, with many issuing EAP guidelines. State dam safety personnel can assist owners to develop EAPs that follow all federal and state regulations specific to their dams.

- Contact information for State Dam Safety Offices and EAP regulations can be accessed at www.damsafety.org/states.
- Sample state EAP guidelines (issued by the New Jersey Department of Environmental Protection, Bureau of Dam Safety and Flood Control) can be accessed at www.nj.gov/dep/damsafety/docs/eapform.pdf.

NIMS Incident Command System (ICS) Forms—such as ICS 205: Incident Radio Communications Plan and 205a: Incident Communications List—can help aid in the development of EAP notification flowcharts. These and other incident management forms offered by FEMA can be accessed at training.fema.gov/emiweb/is/icsresource/icsforms/.

Hazard-Specific Response Plans

The concept of incident response—preparing for and responding to negative events affecting an organization—has long been the standard for the Dams Sector. Examples of standard practices to ensure continuity of operations during adverse events include emergency action plans, preventative maintenance programs, and contingency plans for operations. However, several types of incidents—including cyber, active shooter, and explosives—escalate quickly and therefore require additional thought and planning specific to the type of hazard to implement a quick and effective response.

Hazard-specific response plans, as a stand-alone plan or an annex to a broader plan, can be effective tools to document the specific roles and responsibilities, requirements, and actions necessary to empower personnel to respond to a security incident without unnecessary delays. Regardless the plan format, protocols included in hazard-specific plans should be consistent with protocols in the organization's other emergency plans. As with all emergency plans, hazard-specific plans should include a schedule for training, exercises, and regular review and update.

In addition to the resources listed below to understand and develop hazard-specific response plans, the Dams Sector Crisis Management Suite includes templates to aid in the development of plans, including those pertaining to cyber incidents, active shooter, explosives, insider threat, and pandemics. All templates can be accessed on the HSIN-CI Dams Portal at hsin.dhs.gov/ci/ds.

Cyber Incident Response Plan

Although cybersecurity in the Dams Sector is primarily focused on the industrial control systems (ICS) (also known as operational technology [OT]) that monitor, automate, and control critical physical processes, such as electric generation and transmission, water level and transport, and physical access control, a cyber incident response plan should include both information technology (IT) and OT computing assets. A cyber incident affecting IT systems could compromise business operations or facilitate theft of sensitive business or customer information, potentially leading to operational compromises and/or significant economic losses. A cyber incident affecting ICS can allow attackers to remotely direct physical processes to cause damage, disrupt operations, or cause collateral damage to essential services and nearby communities. A skilled cyber threat actor can pivot from an IT enterprise network to an OT environment if controls are not fully implemented and monitored.

Cyber incident response plans define specific security incidents the organization expects to encounter, the steps that should be taken to respond to the incident and mitigate damage to the organization, and roles and responsibilities for making decisions and taking response actions. Certain entities must comply with law, regulations, and/or policy directing a coordinated, effective defense against information security threats. Depending on applicable requirements, organizations may choose to develop two incident response plans—one covering the operational network and a separate plan for the corporate network—or a single plan (or mirrored plan) that spans both networks.

Establishing clear procedures for handling cyber incidents is a complex undertaking and, though individualized to an organization's mission, size, structure, functions, and requirements, generally contain the following common elements:

- **Goals and Objectives:** Identify the goals and objectives for the cyber incident response plan. Defining what will be accomplished helps an organization articulate direction and guidance for incident response, including as it relates to overall business or operational objectives.

- **Incident Categorization:** Describe each type of cyber incident the organization expects to encounter, such as data destruction or corruption, malicious code, virus attack, system contamination, or privileged user misuse. Defining each incident type is important for implementing the appropriate recommended response actions.
- **Incident Detection (also called Discovery):** Identify the ways in which each expected incident is identified (e.g., automated analysis tools, system behavior patterns, or suspicious activity awareness) and reported. Outline expectations for personnel when suspicious activity is detected and procedures for reporting such suspicious activity.
- **Incident Notification:** Once an abnormal event is identified, prioritize the event to determine the cause and whether it is a minor system event, if it requires immediate escalation, and if it is a reportable incident. Based on this prioritization the plan should outline who to call when a cyber incident occurs. Internal and external reporting processes and requirements should be considered when developing the notification flowchart, with contact information listed for both during business hours and after hours.
- **Incident Analysis:** Define the procedures to direct the incident management processes for determining the current stage of the incident (e.g., beginning, in process, or concluded), the incident's safety and operational impact(s) on the organization (including its personnel, systems, and operations), and if the incident has the potential to spread to other networks or to outside partners or customers.
- **Response Actions:** Define the response procedures for each type of incident identified in the incident categorization step, including detecting the incident, responding to and analyzing the incident, and updating protocols to prevent the incident from reoccurring. Constraints—including time of the incident, deliberate or accidental power loss, business impact of remediation, and forensic requirements—must be considered when making decisions about response actions.
- **Communications:** Identify the point of contact designated to speak for the organization when an incident occurs, lists of all pertinent external contacts (e.g., media, emergency responders, and agencies and authorities), prepared and vetted statements, reporting chain of command, and vendor contacts for critical ICS components.
- **Forensics:** Define the procedures for cyber forensics, which focuses on collecting, examining, and analyzing data related to an incident, while protecting incriminating evidence for use in legal action against a suspected offender. Locate this data in available logs (e.g., network, server, and workstations), physical components (e.g., hard drives), emails, voicemail, texts, and telephone records.

The following resources are available to owners and operators to understand, develop, and implement a cyber incident response plan:

- The *Cyber Essentials Toolkit* (CISA, 2020) is a set of recommended actions to build cyber readiness, organized into six modules. Chapter 6 focuses on responding to and recovering from a cyberattack. Topic areas include developing an incident response plan and disaster recovery plan, using business impact assessments to prioritize resources and identify systems to be recovered, knowing who to call for help in the event of a cyber incident, and developing an internal reporting structure to communicate to stakeholders. The toolkit can be accessed at www.cisa.gov/publication/cyber-essentials-toolkits.

- *Developing an Industrial Control Systems Cyber Security Incident Response Capability* (Department of Homeland Security [DHS], 2009) provides recommendations to help facilities using control systems to better prepare for and respond to a cyber incident regardless of source. This publication can be accessed at us-cert.cisa.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf.
- National Institute of Standards and Technology (NIST) *Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide Recommendations* helps organizations mitigate the risks from computer security incidents by providing guidelines on how to organize a response capability and respond to incidents effectively. This publication can be accessed at nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
- NERC Critical Infrastructure Protection (CIP) Reliability Standard, *CIP-008-6: Cyber Security—Incident Reporting and Response Planning* specifies requirements for Responsible Entities to mitigate the risk to the reliable operation of the Bulk Electric System as the result of a cyber security incident. The standard can be accessed at www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf.

Active Shooter Response Plan

An active shooter is an individual actively engaged in killing or attempting to kill people in a populated area. In most cases, firearms are the weapon of choice during active shooter incidents, but any weapon (such as a bladed weapon, vehicle, or improvised explosive device) can be used to harm innocent individuals. Often absent a pattern or method to victim selection, these incidents can be unpredictable, evolve quickly, and conclude prior to law enforcement arrival. This necessitates the development of an active shooter response plan (sometimes called an active shooter emergency response plan or a preparedness plan) to help an organization to effectively respond to an active shooter situation in order to minimize loss of life.

Determine if an active shooter response plan will stand alone or be appended to the organization's overarching response plan to coordinate with existing procedures for fire evacuation, severe weather, and bomb threats. Key elements to consider in an active shooter response plan or annex include:

- **Goals and Objectives:** Goals and objectives guide the identification of operational priorities and resources required to achieve a needed capability. Goals are broad statements of what personnel, equipment, and resources should achieve. Objectives lead to achieving goals and determining the actions that participants in the process must accomplish. Topics to address in goals and objectives include notification, evacuation and shelter, access control, response coordination, accountability, communication, and recovery.
- **Prevention:** Proactive steps can be taken by facility personnel to identify and report individuals who may be on a trajectory to commit a violent act. Facility employees should learn the signs of a potentially volatile situation and how to report such signs. Accurate and early reporting allows management to quickly address and correct a problem before it becomes more severe. It is important to note that some behavioral indicators may be legal or constitutionally protected activities and should be supported by additional facts to justify increased suspicion.
- **Response Actions**: Response actions, aligned to the identified goals and objectives, describe how personnel can most effectively respond to an active shooter situation in order to minimize loss of life and damage to operations. Examples of actions include:

- **Notification**: Outline who to call when an active shooter incident occurs in order to support decision making and assist first responder operations. Also include a preferred method(s) and pre-drafted messages for reporting active shooter incidents to those at the facility, those entering the facility, and the responding facility security team and law enforcement officers.
- **Evacuation and Shelter**: Identify emergency escape procedures specific to an active shooter incident, which may differ from other types of hazards. Include where to evacuate and how to evacuate when the primary evacuation routes are unusable. Clearly explain shelter-in-place and lockdown procedures, including the differences between the two. Ensure that the plan supports all local, state, and federal regulatory and statutory requirements, including Americans with Disability Act mandates.
- **Access Control**: Identify who is responsible for initiating lockdown procedures for critical assets, secure buildings, parking lots/structures, and roadways and the steps to initiate such procedures. Expect to provide first responders with a master access key or card to ensure their response is not encumbered by locked doors or gates.
- **Response Coordination:** Identify who is responsible for coordinating with law enforcement and what information will be provided to responders. Pre-coordination with local law enforcement ensures the organization understands and is prepared to provide requested information, such as the location of public announcement systems, two-way communications systems, security cameras, and alarm controls, as well as access to utility controls, medical supplies, and law enforcement equipment.
- **Accountability**: Determine the procedures for ensuring accountability of personnel and visitors. This information will prove vital when coordinating with first responders and communicating with concerned family members.
- **Communications**: Identify who is responsible for communicating the organization's message internally and externally. Providing consistent and accurate information to authorities, employees, family, and the media can reduce the impacts of an active shooter scenario on an organization and its people.

- **Recovery**: Identify the organizations included in the whole community recovery effort, including hospitals, grief counselors, lawyers, and employee assistance providers. Link procedures as applicable to the organization's recovery and/or continuity plans.
- **Training Requirements**: During a rapidly evolving active shooter incident, individuals will have to rely on their own judgment to take action to protect lives, including their own. Train employees to recognize and report suspicious behavior; understand how to avoid the shooter by using designated safe areas, hiding, and barricading themselves in rooms that cannot be locked; and know what to expect when law enforcement arrives in order to mitigate risk during an incident.

The following resources are available to owners and operators to understand develop and implement an active shooter response plan:

- *Active Shooter Emergency Action Plan Guide* (DHS) provides a mechanism to document the initial steps toward creating an active shooter preparedness plan. The guide and associated template can be accessed at www.cisa.gov/publication/active-shooter-emergency-action-plan-guide.

- *Developing Emergency Operations Plans: A Guide for Businesses* (FBI, 2018) includes practical advice on how to collaboratively develop and update emergency plans and procedures, including best practices on preparing for and responding to active shooter incidents. The guide can be accessed at www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view.
- *Planning and Response to an Active Shooter* (Interagency Security Committee, 2021) outlines policy requirements for the development, review, and updating of active shooter preparedness plans, along with the training and exercise(s) that must accompany those plans. The guide can be accessed at www.cisa.gov/publication/planning-and-response-active-shooter-interagency-security-committee-policy-and-best.

Explosive Threat Response Plan

Explosive blast attacks are a favored tactic of terrorists because the components and instructions for making bombs are easily obtained, explosives cause extensive damage in a short period of time, and the dramatic nature of the impact generates the attention desired by the attacker. Improvised explosive devices (IEDs) can appear in many forms, ranging from a small pipe bomb to a sophisticated device capable of causing massive damage and loss of life. The device can be carried or delivered in a vehicle or watercraft; carried, placed, or thrown by a person; delivered in a package; or concealed on the roadside.

Explosive threat response plans instruct individuals and organizations on how to perform organized response actions with an emphasis on safety and minimizing disruption to normal activities. The actions typically occur before law enforcement or medical services personnel reach the site. While explosive threat response plans will vary based on the specific geography and assets at a given facility, common elements of an explosive threat response plan include the following:

- **Incident Categorization**: Describe each type of explosive incident the organization expects to encounter (e.g., bomb threats, unidentified or suspicious items, or an actual explosion). Focus on severe, yet realistic conditions that will stress the organization's capabilities. Include a summary of anticipated impacts (e.g., potential for severe injuries and fatalities, facility damage or destruction, and displacement of affected populations or businesses).
- **Goals and Objectives:** Develop a list of goals and objectives that address capability needs and gaps related to the list of incidents identified in the incident categorization step. Identify existing capabilities that meet the goals and objectives.
- **Response Actions**: Include procedures for supervisors—including primary and alternate levels of authority—and employees to take during each type of explosive incident identified in the incident categorization step. Examples of actions include:
  - **Bomb Threat**: Identify the procedures for documenting and reporting the bomb threat, including questions to ask and information to write down. A bomb threat checklist, available at each workstation, can aid in this process. The plan should include instructions to notify authorities immediately to facilitate decisions about lockdown, search, and/or evacuation.
  - **Unattended vs. Suspicious Item:** Educate employees on the differences between an unattended item (item of unknown origin and content with no obvious signs of being suspicious) and a suspicious item (any item reasonably believed to contain

explosives, an IED, or other hazardous material). Identify the procedures for actions to take when encountering such an item, including notifying authorities immediately with information about the location of the item and why it appears suspicious.

- **Search Procedures:** Identify the procedures for conducting a threat assessment to determine the risk level of the possible threat, which determines the need to search for the item. Outline how personnel will conduct the search, including directing the search team to check for items out of place or unusual odors or sounds and directing staff to complete a visual scan of their workspace for primary and secondary devices.
- **Notification**: Identify who to call to support decision making for incident response and continuity of operations when an explosive incident occurs. Include notification protocols to employees, other occupants of the property's building(s), 9-1-1, local hospitals, and federal law enforcement. Pre-drafted messages should be worded to be effective without causing panic and should include instructions about evacuating, sheltering in place, or avoiding certain areas.
- **Lockdown and Evacuation**: Based on the threat assessment, outline the procedures to conduct a full or partial lockdown and/or evacuation. Identify evacuation routes and assembly areas, including backup options in the event the primary options are compromised by the incident. Plan to search and clear the routes and areas prior to directing their use. Identify procedures for directing personnel to reoccupy the site.
- **Response Coordination:** Identify who is responsible for coordinating with law enforcement and emergency medical services should the incident warrant a response and what information will be provided to responders.
- **Accountability**: Determine the procedures for ensuring accountability of personnel and visitors. This information will prove vital when coordinating with first responders and communicating with concerned family members.

The following resources are available to owners and operators to understand develop and implement an explosive threat response plan:

- *DHS-DOJ Bomb Threat Guidance* is a quick reference guide that provides decision makers with response considerations, including pre-threat preparation, threat assessments, staff response actions, and evacuation and shelter-in-place directions. The guidance can be accessed at www.cisa.gov/publication/dhs-doj-bomb-threat-guidance.
- *Bombing Prevention Resources: Bomb Threat Management, Bomb Threat Training, and Awareness Materials* (DHS TRIP*wire*) includes checklists, posters, videos, and cards to help direct the quick and safe response to a bomb threat. Resources available to aid in developing response procedures include *Bomb Threat Checklist*, *Unattended vs. Suspicious Items Poster and Card*, *VBIED Identification Card*, and *Bomb Threat Preparedness and Response Training*. Products can be accessed at tripwire.dhs.gov/node/2001. Training can be accessed at tripwire.dhs.gov/training/376 and tripwire.dhs.gov/training-video-series.
- *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (DHS, 2011) provides guidance to reduce physical damage to structural and nonstructural components of buildings and related infrastructure caused by bomb attacks. The manual can be accessed at www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf.

- *Security and Resiliency Guide: Counter-IED Concepts, Common Goals, and Available Assistance* (DHS, FBI, 2017) assists stakeholders to plan and implement counter-IED activities, including developing a response plan, within their overall public safety and emergency management approach. The guide can be accessed at www.cisa.gov/publication/security-and-resiliency-guide-and-annexes.

Crisis Communications Plans

The initial phase of a crisis can be characterized by confusion, uncertainty, and intense media interest. Information is usually incomplete, and the facts often scattered. The organization's communicators and decision makers will be required to collect information about what happened, separate fact from rumors, activate communication response, and coordinate with other responding agencies. Situational awareness is at a premium, with few second chances to get communication right during this phase of a crisis.

Principles of effective crisis communication:

- Provide timely and accurate facts, including where the crisis occurred.
- Say what is being done now.
- Give credible answers regarding the magnitude of the crisis, including possible threats to the public.
- Share the possible duration of the crisis.
- Explain as much as you can about who will fix the problem, and when.

Crisis communications plans enable the organization to proactively establish effective and consistent communication with affected stakeholders by explaining how the organization will handle a specific crisis. This type of communication is different from risk communication, which increases stakeholder awareness of the general risks posed by dams to help inform community preparedness for emergencies. While both types of communication are important, this handbook focuses on planning for communicating once an emergency takes place.

Elements of a Crisis Communications Plan

Activation Criteria. Define the circumstances under which the plan will be activated and who is responsible for taking action to activate the plan. Consider the possibility of a worst-case yet realistic scenario.

Procedures. The crisis communications plan is not a step-by-step or how-to document and therefore should not be overly long or detailed. The plan should provide a basic, general structure that can be adapted to emergency response situations, including procedures to assist with making decisions and disseminating information. Examples of procedures include the following:

- Internal and external communication actions the organization will take to disseminate key messages, including when and how the messages will be released.
- Information clearance to ensure information is accurate while aiming to release it quickly.
- Tools and mechanisms used to facilitate communications, including via phone, email, intranet, website, and social media feeds.
- Secure the space, equipment, and personnel necessary to operate the public information and media operation during an emergency 24-hours-a-day, 7-days-a-week, if needed.

Audiences. Identify potential audiences that will need information during and following an incident, including employees and their families, customers and suppliers, organization leadership, government officials, communities, and members of the media. Ensure that this list includes audiences receiving messages that are required by law or regulation and those partners the organization will need to support the response effort (e.g., first responders, evacuation centers, and non-governmental organizations).

Key Messages. Develop messages to be used in response to potential scenarios the organization could face. Pre-scripted messages can be tailored during an actual incident based on what the intended audience needs to know and through what mechanism(s) they are accessing the information. Messages should include a brief description of what happened, a timetable for future actions, and suggested actions the intended audience should take. Depending on when the messages are released and to whom (i.e., internal or external audience), the details of these messages may vary. Ensure appropriate personnel (e.g., managers or the legal department) review and sign-off on all messages prior to release.

Roles and Responsibilities. List the members of the crisis communication team and their roles and responsibilities in carrying out the plan. At a minimum, identify a primary and backup individual responsible for serving as the spokesperson, fielding media calls, and communicating internally with employees. Include and maintain an updated contact roster for all team members and ensure team members receive regular media training to effectively carry out their duties.

Supporting Information. Include all other information necessary to effectively and efficiently implement the plan, including contact information for various audiences, call logs, checklists, forms, templates, site and building diagrams, fact sheets, and associated plans and policies.

Considerations when Developing a Crisis Communications Plan

Communications Principles

Crisis communication is most effective when guided by the principles of planning for communication, maintaining trust in the organization's response to the crisis, ensuring consistent and transparent messaging, acknowledging uncertainty or assumptions, and respecting the audience's concerns. This means presenting information that is simple, credible, accurate, consistent, and delivered on time. Keep these principles in mind as the organization is developing procedures and messaging.

Coordination with Other Plans

Communications protocols underpin each phase in an emergency. As the crisis communications plan is developed, ensure the protocols and contacts are consistent with those of the other planning documents, especially the notification and communications procedures within the EAP.

Establish Contact Lists

Dam safety is a shared responsibility. While dam maintenance and operation are the responsibility of the owner, local officials and the public are also responsible for awareness and preparedness. In most cases, the EAP will dictate the protocols for timely notification of those responsible for taking emergency actions, including communication with the community and other stakeholders. For the purpose of the crisis communications plan, maintain updated contact lists and working relationships for the following entities:

- **Public Information Officers:** Develop working relationships with the local law enforcement agency, emergency management agency, fire department, emergency medical services provider, and FBI Field Office. Discuss who to contact during emergencies and develop a standardized communications plan to ensure all responding agencies can communicate during an emergency impacting the facility and community (e.g., establish a common radio frequency, determine common terms for actions and locations, and coordinate public messaging).

- **Media Outlets (print and broadcast):** Knowing who to call and establishing trust during steady-state operations can help the organization more quickly disseminate accurate information. Determine how best to deliver press releases for public release and identify media staging locations outside potential impacted areas.
- **Evacuation Sites and Healthcare Facilities:** Determine who to contact and notification procedures for supporting the response efforts, including schools and public venues for evacuations and hospitals and morgues for receiving the injured and casualties.

Train to Communicate Effectively

Given the criticality of communication during an incident, organizations should include internal and external communications protocols in training and exercises. Invite the organization's public affairs official(s) to emergency training and exercises and train managers and emergency personnel on how to communicate effectively.

Evaluate and Update the Plan

The single most important communication responsibility that can be assigned to someone in the organization is the duty to keep the plan current. Schedule an annual review of the plan and update it as necessary. When the plan is used for a crisis, evaluate the performance of the plan, document lessons learned, and determine specific actions to improve crisis systems or the crisis plan. Failure to incorporate lessoned learned from the crisis increases the chance of a failed response in the future.

Resources for Developing a Crisis Communications Plan

The Dams Sector Crisis Management Suite includes templates to aid in the development of crisis management plans, including communications plans. All templates can be accessed on the HSIN-CI Dams Portal at hsin.dhs.gov/ci/ds.

Crisis and Emergency Risk Communication (CERC): Crisis Communications Plans (Centers for Disease Control [CDC], 2014), developed by the CDC CERC program, is one chapter of the CERC Manual focused on developing a plan and implementing it during the various phases of a crisis. While the program is focused on public health emergencies, the crisis communications and plan principles apply broadly across all hazards. CERC program materials can be accessed at emergency.cdc.gov/cerc/.

Crisis Communications Quick Reference Guide (FBI) is a checklist for public information officers and responders to use in preparation for and response to an incident. The checklist includes several categories of considerations while developing a crisis communications plan, including pre-event actions, coordinating press conferences, and actions to take at the onset of an incident. The guide can be accessed at www.dhs.gov/sites/default/files/publications/fbi-crisis-communications-trifold-reference-guide.pdf.

Ready Business: Crisis Communications Plan presents several categories of information to include in a crisis communications plan, including detailing the intended audiences, pre-scripting messages, and leveraging information and resources to support the plan. This resource can be accessed at www.ready.gov/crisis-communications-plan.

Recovery Plans

> **Recovery Plans**
>
> Dams Sector organizations may use the terms "recovery plan" or "rapid recovery plan" to refer to the same type of document. Some include the equivalent of a recovery plan as a section of another document, such as an emergency action plan. This handbook uses the term recovery plan as a generic, encompassing term to refer to any of these documents.

Certain dam projects, especially some large federal dams, provide a wide range of economic, environmental, and social benefits to a broad community. These benefits can include irrigation, electric power generation, "black start" capabilities, water storage, recreation, navigation, flood mitigation, and control of sediment/hazardous materials and mine tailings. Disruption of such projects for extended periods of time could devastate regional or national economies. While not necessarily providing the same level of regional or national benefits, disruptions at smaller dams may extensively impact the local community and dam owner. A recovery plan can be essential for delivering project benefits by quickly repairing damage to at least partially restore project functions and preparing for long-term repairs to fully restore the project.

The primary objective of a recovery plan is to efficiently restore the dam project to a functional condition. To accomplish this objective, the organization must address the hazards likely to impact each critical component of the facility and its operations (e.g., natural, accidental, or intentional) and plan to mitigate impacts and restore project function in collaboration with the response phase to minimize economic losses. The close collaboration between the response and recovery phases means that some concepts listed in this chapter may fall within an organization's response plan. Absent the existence of a response plan, immediate and short-term recovery actions can be included in a recovery plan.

The development of a recovery plan starts with identifying the facility's critical components and the type of hazard(s) likely to damage each component, then describing the magnitude of damage expected. Based on the probable damage estimation, the organization develops a list of short- and long-term options to minimize consequences (e.g., procurement of equipment or supplies, agreements with vendors for rental equipment or repairs, and communication with relevant authorities). This analysis of components concludes with documenting the recommended actions from the list of options most likely to limit the magnitude of the consequences. Other elements of a recovery plan document the internal emergency response actions critical to the success of the recovery phase, such as communication, reference materials, and meals and lodging.

Implementation of the recovery plan should begin as soon as possible after the catastrophic event (e.g., dam failure, loss or damage to a powerhouse, or loss of main transmission line). The recovery phase can overlap with actions taken during the response phase to return the dam to service. Recovery phases include "initial" (within one week) and "long-term" activities (recovery could continue for months), depending upon the magnitude of impact on facility operations (e.g., dams, powerhouses, and water conveyance).

Elements of a Recovery Plan

Hazard Identification. The first step in developing the recovery plan is to identify the hazards (e.g., ballistic damage to shell and windings or trunnion pin failure) likely to impact each critical component at the facility (e.g., switchyard transformer or tainter gates). A universe of potential hazards (sometimes called emergency scenarios) need not be listed for each facility. Focus this step on

developing a list of scenarios tailored to the site specifics of the facility. For example, an organization may choose to omit overtopping from the recovery plan because the facility is designed to accommodate flows over the entire structure. Other organizations may include possible loss of project function caused by interruption of communications links or by cyberattacks that make the automated control system inoperable.

Existing dam safety tools (e.g., the PFMA approach) can be used as inputs to develop emergency scenarios. However, the PFMA process may not cover all scenarios applicable to a facility, such as manmade threats. Organizations should leverage other inputs (e.g., the tools listed in the Understand Hazards chapter of this guide) to develop the list of hazards impacting critical components.

Consequence Estimate. For each component assigned a hazard type, describe the magnitude of damage expected. Focus the description on the facility's ability to deliver project functions, including primary concerns about the damage and ability to mitigate, caveats and assumptions about the estimate, and expected level of service while mitigation actions are underway.

Mitigation Options and Recommended Actions. Develop a list of options to minimize the consequences described, either by reducing initial damage, limiting the progression of the initial damage, or reducing the time necessary to repair the damage. Focus these repair/replacement options on the organization's actions to restore full or partial function, such as procuring materials and equipment; stockpiling materials; and identifying local equipment repair contractors, suppliers of key materials and equipment, and providers of rental equipment or heavy transport. Options can also include relying on existing capacity until other recovery measures can be taken.

Highlight the recommended action for each hazard, selected from the list of options as most likely to limit the magnitude of the consequences. Describe the rationale for selecting that option and any caveats or assumptions for the decision. Final selection of the recommended actions during an actual emergency will be dependent on the severity of the damage, availability of materials and equipment, and other factors that may impact the assumptions that underpin the initial analysis.

Coordination with Internal Emergency Response. Because the recovery phase usually overlaps with the response phase, consider the following internal emergency response actions that could aid in returning the dam to service. Include procedures on these actions in the recovery plan, as appropriate.

- **Communications:** Describe how communication will occur throughout the emergency, including alternate communications sources to account for the possible loss or interruption of communications links.
- **Reference Materials:** Include the maps, drawings and specifications, original design documents, and photographs that would be useful in responding to an emergency in the body of the plan or as an appendix. Ensure rapid access to this information.
- **Vehicles, Equipment, Materials, and Contractors:** List the vehicles, materials, and equipment required to respond to the identified hazards. A current list of contractors and support personnel should also be listed for easy reference.
- **Response Times and Geographical Limitations:** Address the anticipated response times, call-out procedures, and geographic limitations. Using text and graphics, include clearly defined directions to critical areas and other locations important to the response. Security exclusion zones and potential staging areas should also be identified.

- **Meals and Lodging:** List logistical considerations for sustaining personnel detailed to temporary quarters.

Considerations when Developing a Recovery Plan

Coordination with Other Plans

The content of a recovery plan should be coordinated with existing emergency planning documents to minimize redundant content and prevent inconsistencies between plans. Reference associated plans—including section number and title—to eliminate the need to repeat the same information in multiple plans. This approach will make the recovery plan simpler to develop, easier to maintain, and easier to read. It will also help prevent inconsistencies between plans. The following are examples of plans utilized in the Dams Sector that may warrant coordination:

- **Emergency Action Plans:** The recovery plan is designed as a separate document to supplement the primary EAP. Whereas the EAP facilitates early warning and evacuation of potentially affected downstream areas, the recovery plan provides guidance to respond to incidents, mitigate impacts, and perform emergency repair of affected company structures and plant facilities. The recovery plan should be consistent with the content and guidelines in the EAP to ensure site personnel conducting recovery operations understand the objectives and instructions.
- **Portfolio of Dams:** A recovery plan should be prepared on a site-specific basis to address considerations to bring that facility back into operation as efficiently as possible. However, it may be possible and advantageous to develop a single plan applicable to a portfolio of dams with similar components or along the same river system. When multiple-project recovery plans are used, include issues unique to an individual dam in a separate appendix.

Financial Information

Major recovery activities depend on available funding. When developing the component analysis to determine the types of damage that might be expected and the various repair/replacement options to restore full or partial function, consider also including the probable time and cost for those options. Organized into tables, this data can provide a quick reference to assist decision makers make important decisions quickly during the tense post-incident period.

Sensitive Information

Recovery plans need to be disseminated and easily accessible in case of an incident. However, development of a recovery plan might require use of sensitive information such as specific vulnerabilities and potential consequences. Therefore, sensitive material should be kept separate from the portion of the plan that contains recommendations and courses of action. Sensitive material should only be available to persons with a need to know.

Response Coordination

In the event of major damage to a dam or to other infrastructure, multiple agencies could have significant roles in the initial incident response and in the recovery phase to restore project function. Law enforcement agencies would focus on preserving the site in the post-incident condition to facilitate criminal forensic investigations. In the case of a release of hazardous materials, extensive, long-term clean-up activities involving federal and state environmental, health, and safety agencies may be needed. If extensive project reconstruction is necessary, approvals may be required from

several federal and state permitting agencies. The need for interagency coordination and potentially conflicting priorities among the agencies could complicate the recovery process. Address these possible conflicts in the recovery plan to the extent possible.

Reconstruction Coordination

Reconstruction could require coordination with local authorities and regulatory agencies. To facilitate a quick response, it may be necessary to streamline internal authorities for procurement or contracting.

Training and Exercise

As is the case with all emergency plans, the recovery plan should include training requirements for appropriate personnel and periodic exercises simulating plan implementation. These actions will help ensure designated personnel are familiar with the project's recovery strategy and can develop best practices from lessons learned. Also include a requirement for periodic recovery plan updates to incorporate changing project requirements and best practices.

Internal Maintenance of the Plan

As is the case with all emergency plans, address how the recovery plan will be maintained and updated.

Resources for Developing a Recovery Plan

The Dams Sector Crisis Management Suite includes templates to aid in the development of crisis management plans, including recovery plans. All templates can be accessed on the HSIN-CI Dams Portal at hsin.dhs.gov/ci/ds.

Emergency Operations Planning: Dam Incident Planning Guide (FEMA, 2019) summarizes the concepts that a community should consider when creating dam incident-specific elements of local emergency operations plans, including recovery factors and planning considerations. The guide is available at www.fema.gov/sites/default/files/2020-08/dam_incident_planning_guide_2019.pdf.

FERC Division of Dam Safety and Inspections, *FERC Security Program for Hydropower Projects Revision 3A* includes guidelines for use by its licensees when developing an internal emergency recovery plan to supplement an emergency action plan. The guidelines include a recommended table of contents and a content description for each of the main sections. The guidelines are available at www.ferc.gov/industries-data/hydropower/dam-safety-and-inspections/security-program-hydropower-projects-revision.

Continuity Plans

Continuity planning helps facilitate the performance of an organization's essential functions during any situation that may disrupt normal operations. A continuity plan can encompass a wide range of topics such as functional roles and responsibilities, lines of authorities, alternate personnel and operations locations, logistics support, resource requirements, and systems for managing communication and information flow. While discussing some of these broader aspects of continuity planning, this handbook is focused primarily on those issues that affect continued safe operation of dams and related infrastructure. Reference the resources listed at the end of this chapter for additional information on other elements of a continuity plan.

Continuity Planning

The definition of continuity of operations (COOP) planning varies from organization to organization. COOP can refer to a complete continuity program, covering all interrelated aspects of continuity, or can refer to business continuity for an organization in the absence of key personnel. This handbook refers to continuity planning as it relates to the continued safe operation of a dam.

The scale of an organization's operations will dictate if one continuity plan will be sufficient or if multiple, discrete plans should be developed into a comprehensive continuity program. Continuity plans could be developed for escalating operations in the event of a natural disaster or manmade incident, black start contingencies, civil unrest, pandemics, labor unrest, or physical or cyber security breaches. These elements can be broken into separate plans or part of an overall continuity program. Regardless of the scope of the continuity plan or program, implementation of the continuity plan is conducted in four phases:

1. Readiness and preparedness to develop, review, and revise continuity plans
2. Activation of plans, procedures, and schedules for the continuation of essential functions
3. Continuity operations to perform essential functions, account for personnel, establish communications capabilities, and prepare for reconstitution
4. Reconstitution to resume normal operations

Elements of a Continuity Plan

Identification of Essential Functions. Essential functions are the limited set of organization-level functions that should be continued throughout or resumed rapidly after a disruption of normal activities. The identification and prioritization of essential functions is the foundation for continuity planning because the functions enable the organization to provide vital services, exercise civil authority, maintain the safety of the community, and sustain the economic base during an emergency. Each organization should identify its essential functions as part of continuity planning, such as those functions pertaining to the safe storage or release of water:

- Controls and systems that open or close gates and valves
- Personnel who manipulate those systems and controls
- Personnel who decide when and how much to adjust release of water
- Dam safety engineers authorized to make decisions on the safety of the dam
- Collection of data that forms the basis of such decisions
- Communication between those operating the controls and those deciding on releases

Interoperable Communications. Continuity of communications capabilities could become an issue during a crisis for any number of reasons, with disruptions of phone systems (landline and cell) even more prevalent during certain emergency situations. In addition, the crisis-related relocation of specific functions to alternate facilities can contribute to disruptions in communications systems and computer networks at a time when reliable communication is most vital. Continuity plans should focus on maintaining critical communications capabilities and what to do when that is not possible.

Delegations of Authority. Certain types of emergency situations might cause the temporary or permanent loss or incapacitation of key personnel, resulting in the loss of communication within the organization. Continuity plans should clarify what decision-making authority will be transferred under various circumstances. For example, if communication with the chief hydrologist is disrupted, will an onsite supervisor be expected to open gates after a heavy rain? As part of developing the plan, it is also necessary to clarify who has the authority to commit resources and sign emergency contracts.

Alternate Facilities. Continuity plans typically address the relocation of essential functions if the primary location for operations has been disrupted. In the Dams Sector, while it is not possible to relocate the actual dam infrastructure, relocation of some support functions may apply. Review the organization's essential functions and identify alternate facilities for operations where appropriate.

Vital Records. Recognizing that some data might become unavailable—due to computer network malfunction, loss of communications capabilities, sensor failures, and disruption in National Weather Service systems—continuity plans should focus on methods to maintain access to critical information and alternatives when information is not available. At a minimum, vital records planning should consist of information deemed critical to maintaining safe water levels in the reservoir and downstream, including reservoir levels, stream-flow data upstream and downstream of a dam, expected near-term inflows, and release rates for various gate positions.

Human Capital. Continuity plans should describe how to maintain essential functions in case of serious disruption to staffing caused by events such as a highly contagious disease, a natural disaster in a surrounding area, or a biological or chemical incident. Planning should identify the number of people and skills required to support essential functions, mapped to the potential availability of those within and outside of the organization who could fill in during emergency situations. Consider the development of mutual aid agreements or contract agreements for the use of temporary personnel from outside the organization.

In addition to planning for disruptions to staffing, pay attention to planning for the retirement or non-availability of personnel with critical institutional knowledge of the facility and its operations. Succession planning can take the form of identifying personnel who have demonstrated their capabilities and could move into positions of greater responsibility and authority with appropriate training and guided experience.

Considerations when Developing a Continuity Plan

Sensitive Information

Continuity plans need to be disseminated and easily accessible in case of an incident. However, development of a continuity plan might require use of sensitive information such as personnel data and sensitive location information. Sensitive material should be kept separate from the portion of the plan that contains recommendations and courses of action. Sensitive material should only be available to persons with a need to know.

Coordination with Other Organizations

Should the impacts of the emergency extend beyond the organization's property and/or capabilities, coordination with other entities in the surrounding community will be necessary to effectively plan for and recover from the incident. Coordination on the following items can be integrated into an organization's continuity planning process:

- Incorporate capabilities of other entities into the organization's planning and exercises
- Coordinate risk assessments to identify threats and hazards relevant to the organization's mission and the location(s) where essential functions are performed
- Coordinate emergency, shelter-in-place, and regional and local evacuation plans
- Participate in alert and notification networks and access control initiatives
- Identify interdependencies and ensure critical infrastructure resilience at all levels
- Coordinate awareness of continuity resources and security requirements

Resources

People, communications, facilities, infrastructure, and transportation resources are necessary for the successful implementation of an organization's continuity program. During planning, organizations should identify the human resources, equipment, training, facilities, funding, materials, technology, and information needed to plan for and reconstitute operations after an incident. Consider all potential sources, including internal resources, mutual aid agreements, grants, and procurement.

Absenteeism

A natural hazard, pandemic, or incident (whether intentional or not) affecting a community, region, or the Nation could result in high degrees of worker absenteeism. Employees may be absent because they are ill, incapacitated, providing care to family members, unwilling to go to work for fear of becoming ill, or lacking transportation. Absenteeism of a short duration may be manageable, but expectations of longer durations may require response actions, such as the following:

- Identify and assess essential services, functions, and processes
- Review equipment and assets critical to support each essential function
- Determine the most effective ways to ensure an adequate supply of essential materials
- Identify the types and number of workers critical to sustain essential functions
- Identify human resource and protective actions to sustain essential workforce
- Identify interdependent relationships and take actions to sustain those essential supports
- Identify federal, state, and local regulatory requirements that may affect facility operations
- Identify effects from mitigation strategies and take actions to reduce negative impacts

Training and Exercise

Training and exercises should assess and validate continuity plans, policies, procedures, systems, and alternate locations. Initial and recurring training programs inform and familiarize leaders and staff with continuity plans and procedures. Exercise programs consisting of both planned and short/no-notice events improve an organization's preparedness posture and emphasize the value of integrating continuity functions into daily operations.

Resources for Developing a Continuity Plan

The Dams Sector Crisis Management Suite includes templates to aid in the development of crisis management plans, including continuity plans. All templates can be accessed on the HSIN-CI Dams Portal at hsin.dhs.gov/ci/ds.

The *Continuity Resource Toolkit* (FEMA, 2018) provides public and private sector partners with tools, templates, and resources to help implement concepts found in the Continuity Guidance Circular, including developing and maintaining a successful continuity program and plan. The toolkit can be accessed at www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit.

NFPA 1600: Standard on Standard on Continuity, Emergency, and Crisis Management (NFPA, 2019) provides the fundamental criteria for preparedness and resilience, including the planning, implementation, execution, assessment, and maintenance of a continuity program. The standard can be accessed at www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600.

Exercises

Although emergency incidents at dams and/or dam failures are uncommon, training and exercises are necessary to maintain operational readiness, timeliness, and responsiveness in the event that an incident does occur. Exercises also provide the necessary verification, training, and practice to improve the EAP and the operational readiness and coordination efforts of the whole community (i.e., all parties responsible for responding to emergencies at a dam). Periodic exercises, conducted on a pre-determined schedule or after an incident, result in an improved EAP because lessons learned are incorporated into the updated planning document(s). Beyond testing the EAP, exercises can yield the following benefits for an organization's crisis management program:

- Raise the general awareness of the hazards likely to impact the organization.
- Reveal the strengths and weaknesses of the plan(s) selected for testing, including identifying deficiencies in resources, information and data available, and protocols.
- Ensure key staff members, emergency management agencies, and other senior leaders understand their roles and responsibilities and improve individual performance of those responding to the crisis.
- Improve coordination efforts between the dam owner and emergency management authorities potentially responding to incidents at the dam project.
- Identify improvements to the plans and future training and exercises to enhance the organization's ability to respond to an incident.

Several types of exercises, as defined below, are generally used to build and test plans in a crisis management program. The specific type is selected based on the intended outcome of the exercise, as explained in the descriptions. Owners and operators within the Dams Sector may have different definitions of these exercise types stemming from their organizational processes. Exercise programs do not have to include all types of exercises. However, robust exercise programs build complex exercises by combining multiple exercise types.

Although the exercise types will vary significantly in terms of scope and scale, the same general framework can be applied when planning most of the exercise types.

- **Define the Purpose and Scope of the Exercise:** A clear definition of the need for the exercise and the purpose for conducting it will aid the planning process by clarifying who should be involved and the exercise scope (e.g., tabletop, game, or full-scale). This should stem from a whole community approach, with input from senior leaders across organizations and jurisdictions.
- **Assemble the Planning Team:** The size of the planning team and representation on it depends on the scope of the exercise. The team should include, at a minimum, personnel from the facility involved in the exercise, local law enforcement, and first responders.
- **Develop the Scenario:** The planning team's initial task is to develop the exercise scenario, which should be a plausible event scaled to the purpose of the exercise. This step should stem from a whole community approach, with input from senior leaders across organizations and jurisdictions.

- **Develop Exercise Guidelines:** Depending on the type of exercise and the scenario, the planning team should describe any limitations placed on the design, development, and implementation of the exercise. Limitations include the ability of responders to participate, lengthy authorization protocols, areas off-limits for safety reasons, or financial constraints.
- **Build Master Scenario Events List:** The Master Scenario Events List (MSEL) developed by the planning team lists the exercise messages and key events used to fully play out the scenario. The MSEL specifies the time a message is expected to be delivered, who delivers it to whom, a message number, and a short description of the message.
- **Prepare Exercise Materials and Evaluator Guides:** Participants should receive invitation letters and other exercise materials describing the exercise purpose and goal; scenario descriptions pertaining to their role; and safety, health, and logistics plans. Equally important is developing the guidelines for the observers who will evaluate actions and decisions as the exercise unfolds.
- **Complete Post-Exercise Evaluation:** Post-exercise evaluations provide the basis for improving the plans or procedures that were tested as part of the exercise. An effective evaluation assesses performance against exercise objectives and identifies strengths and areas for improvement. Evaluation is important and considered in all phases of the exercise planning cycle.
- **Execute Improvement Plans:** Improvement planning activities can help shape priorities and support continuous improvement. Actions identified during improvement planning help to strengthen the whole community in its ability to plan, organize, equip, train, and exercise. Any actions intended to improve future exercises should apply the SMART concept, which ensures that corrective actions are developed to be *Specific, Measurable, Achievable, Relevant, and Time-bound*.

Types of Exercises

Discussion-Based Exercises

Discussion-based exercises familiarize participants with current plans, policies, agreements, and procedures. They may also be used to develop new plans, policies, agreements, and procedures. As the name implies, discussion-based exercises typically include a presentation of the scenario, followed by a facilitated discussion. The following are types of discussion-based exercises:

- **Seminar:** Seminars generally provide an overview of authorities, strategies, plans, policies, procedures, protocols, resources, concepts, and ideas. As a discussion-based exercise conducted in a low-stress environment, seminars can be valuable for entities when developing or making major changes to existing plans or procedures. Seminars can be similarly helpful when attempting to assess or gain awareness of the capabilities of interagency or inter-jurisdictional operations. During this type of exercise, information is conveyed through various instructional techniques, including lectures, multimedia presentations, panel discussions, and case study discussions.
- **Workshop:** Although similar to seminars, workshops differ in two important aspects: participant interaction is increased and the focus is placed on a specific topic, such as achieving or building a product. Effective workshops entail the broadest attendance by relevant stakeholders to obtain new or different perspectives with the goal of solving complex issues or obtaining consensus. Products produced from a workshop can include

new standard operating procedures, emergency operations plans, continuity of operations plans, or mutual aid agreements. During this type of exercise, a presentation or briefing conveys the background for the workshop and then facilitated breakout sessions focus discussions on specific issues.

- **Tabletop Exercise:** A tabletop exercise (TTX) is intended to generate discussion of various issues regarding a hypothetical, simulated emergency. TTXs can be used to enhance general awareness; validate plans and procedures; rehearse concepts; and/or assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined incident. Generally, discussions during TTXs facilitate conceptual understanding, identify strengths and areas for improvement, and/or achieve changes in perceptions.
- **Games:** A game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedures designed to depict an actual or hypothetical situation. Games explore the consequences of player decisions and actions, which can be useful when validating plans and procedures or evaluating resource requirements.

Operations-Based Exercises

Operations-based exercises validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps in an operational environment. These exercise types will typically include real-time responses, such as initiating communications or mobilizing resources. The following are types of operations-based exercises:

- **Drills:** A drill is a coordinated, supervised activity usually employed to validate a specific function or capability, measured against established standards, in a single agency or organization. Drills are commonly used to depict a realistic environment to provide training on new equipment, validate procedures, or practice and maintain current skills. Drills can also be used to determine if plans can be executed as designed, to assess whether more training is required, or to reinforce best practices.
- **Functional Exercises:** Functional Exercises (FEs) are designed as lengthy and complex, to validate and evaluate capabilities, multiple functions and/or sub-functions, or interdependent groups of functions. FEs are typically focused on exercising plans, policies, procedures, resources, and personnel involved in management, direction, command, and control functions. In FEs, events are projected through an exercise scenario with event updates that drive activity typically at the management level. An FE is conducted in a realistic, real-time environment to facilitate decision making; however, movement of personnel and equipment is usually simulated.
- **Full-Scale Exercises:** Full-Scale Exercises (FSEs) are typically the most complex and resource-intensive type of exercise, designed to challenge the system under review in a highly realistic and stressful environment. FSEs involve multiple agencies, organizations, and jurisdictions and validate many facets of preparedness, including pinpointing resource and personnel capabilities, revealing planning and resource shortfalls, and testing inter- and intra-organizational coordination. All decisions and actions by players occur in real time and generate real responses and consequences from other players. The exercise messages may be scripted or visual and involve staged scenes, props, and role-playing victims.

Considerations when Conducting Exercises

Coordination with External Stakeholders

Dam owners should include the whole community—including state, local, and tribal emergency authorities—in site visits and exercise activities. This coordination could also extend to other dam owners within the same drainage basin because incidents often have cascading effects. Coordination with these external organizations can help ensure their familiarity with the dam location, access routes, key features, and potential incident impacts. Involving relevant organizations and agencies will not only maintain plan familiarity among the participants, but differing viewpoints can help identify possible deficiencies of the plan(s) being exercised.

Clearly Defined Objectives and Outcomes

Critical to the success of exercises, regardless the type, is preparation of participants. Prior to the exercise, utilize a pre-brief conference call and/or read-ahead material to educate participants on exercise objectives, policies and procedures leveraged during the exercise, and intended outcomes (e.g., product or goal). A pre-brief can also save time on the day of the exercise by reviewing administrative items, such as how the exercise will be carried out, the time period to be simulated, and ground rules and procedures. Objectives, policies and procedures, and outcomes can be documented in a Situation Manual (for discussion-based exercises) or an Exercise Plan (for operations-based exercises).

Exercise Frequency

Regularly exercised crisis management plans ensure that those involved in implementation do not lose familiarity with their roles and responsibilities and that resources, equipment, and protocols remain valid. Dam owners/operators, in consultation with emergency management authorities and in compliance with any requirements, should determine the exercise types and frequencies appropriate for their dams. The owner/operator may choose to implement a formal exercise program inclusive of multiple exercise types that are conducted in an ascending order of complexity and scheduled with enough time to incorporate lessons learned between exercises. The following list depicts four exercise types listed in order of complexity:

- Seminars with primary emergency management authorities
- Drill to test the EAP notification flowchart and emergency equipment/procedures
- Tabletop exercise
- Functional exercise

A full-scale exercise should be considered when there is a need to evaluate actual field movement and deployment. When a full-scale exercise is conducted, safety is a major concern because of the extensive field activity. If a dam owner has the capability to conduct a full-scale exercise, commit to schedule and conduct the entire series of exercises listed above before conducting the full-scale exercise. At least one functional exercise should be conducted before conducting a full-scale exercise. Functional and full-scale exercises should also be coordinated with other scheduled exercises, whenever possible, to share emergency management resources and reduce costs.

Post-Exercise Evaluation

Emergency exercises and equipment tests should be evaluated orally and in writing. An after-action review should be conducted immediately after an exercise or actual emergency, with all involved parties identifying strengths and deficiencies in the planning documents. The after-action review

should focus on procedures and other information in the plan (e.g., outdated telephone numbers on the notification flowchart; inaccurate inundation maps; and problems with procedures, priorities, assigned responsibilities, materials, equipment, or staffing levels). Participants in the after-action review should discuss and evaluate the events before, during, and after the exercise or actual emergency; actions taken by each participant; the time required to become aware of an emergency, initiate communications, and mobilize resources; and improvements for future emergencies.

The outcome of the after-action review is an After-Action Report / Improvement Plan (AAR/IP), which generally includes an exercise overview, analysis of capabilities, and an overview of performance (including a list of corrective actions) related to each exercise objective and associated capabilities. Corrective actions captured in the AAR/IP should be tracked and continually reported on until completion. Any plan revised as a result of the exercise should be disseminated as appropriate.

Resources for Conducting Exercises

The DHS Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs and a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Available templates allow an organization to design and develop an exercise more easily and consistently. The HSEEP methodology and associated templates for conducting exercises can be accessed at www.fema.gov/hseep.

The Dams Sector Tabletop Exercise Toolbox (DSTET), a component of the Dams Sector Crisis Management Suite, provides dam owners and operators with an exercise-planning tool that provides the materials needed to conduct a discussion-based exercise using one of five scenarios: general physical security threat, active shooter, international adversary threat, cyber incident (insider threat), and cyber incident (external adversary). Consistent with HSEEP, DSTET materials—including a situation manual, briefing slides, facilitator and evaluator handbook, planning guide, and feedback forms—can be tailored by the organization to meet their exercise needs. The DSTET is available by contacting the Dams Sector Management Team at DamsSector@cisa.dhs.gov.

CISA offers a broad-range of exercise related services to critical infrastructure partners, including end-to-end planning and execution of discussion-based and operational exercises. These exercises provide stakeholders with effective and practical mechanisms to examine plans and procedures, potentially identify areas for improvement, and share best practices. These exercises may also inform future planning, technical assistance, training, and education efforts. For more information, or to request an exercise, contact CISA Exercises at CISA.Exercises@cisa.dhs.gov.

The following documents outline suggested or required content (depending on the document) for dams-related exercises. Non-regulated entities may consider reviewing the requirements and voluntarily implementing provisions relevant to their operations, as an industry best practice. Links to access these requirements can be found in Appendix B. Bibliography.

- *FEMA P-64: Emergency Action Planning for Dams* (FEMA, 2013) highlights the importance of exercising the EAP and includes details about types of EAP exercises, frequency of exercises, and procedures for evaluation.
- *Engineering Guidelines for the Evaluation of Hydropower Projects, Chapter 6 Emergency Action Plans* (FERC, 2015) outlines the requirements for FERC licensees related to EAP exercises, including exercise type and frequency.

- The following NERC CIP Reliability Standards list requirements for Responsible Entities to exercise their Bulk Electric System (BES) cyber incident response and recovery plans including exercise type and frequency:
  - CIP-003-8: Cyber Security—Security Management Controls
  - CIP-008-6: Cyber Security—Incident Reporting and Response Planning
  - CIP-009-6: Cyber Security—Recovery Plans for BES Cyber Systems

Appendix A: Acronyms and Abbreviations

BES	Bulk Electric System
CDC	Centers for Disease Control and Prevention
CERC	Crisis and Emergency Risk Communication
CIP	critical infrastructure protection
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Comprehensive Preparedness Guide
DHS	Department of Homeland Security
DSTET	Dams Sector Tabletop Exercise Toolbox
EAP	emergency action plan
ERP	emergency response plan
FBI	Federal Bureau of Investigation
FE	functional exercise
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FSE	full-scale exercise
HSIN-CI	Homeland Security Information Network—Critical Infrastructure
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Incident Command System
ICS	industrial control system
IED	improvised explosive device
IT	information technology
MSEL	master scenario events list
NDSP	National Dam Safety Program
NERC	North American Electric Reliability Corporation
NFPA	National Fire Protection Association
NID	National Inventory of Dams
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
OT	operational technology
PFMA	Potential Failure Modes Analysis
TRIP*wire*	Technical Resource for Incident Prevention
TTX	tabletop exercise
VBIED	vehicle-borne improvised explosive device

Appendix B: Bibliography

DHS and CISA provide the following tools and resources to support implementation of this Handbook. The tools and resources are for informational and educational purposes, and DHS/CISA does not guarantee their content or endorse any specific person, entity, product, service, or enterprise. The tools and resources identified do not encompass all tools and resources. Tools and resources requiring a paid subscription and/or organizational membership are identified with an asterisk (*). The use of any paid tool or resource is at the discretion of the organization.

*ASIS International. *ASIS ORM.1:2017: Security and Resilience in Organizations and their Supply Chains Standard*, March 2017. Accessed July 13, 2021. https://www.asisonline.org/publications--resources/standards--guidelines/orm/.

Association of State Dam Safety Officials. Access State Dam Safety Programs & Contacts Webpage. Accessed July 13, 2021. https://www.damsafety.org/states.

Centers for Disease Control and Prevention, Crisis and Emergency Rick Communication (CERC). *CERC: Crisis Communication Plans*, 2014. Accessed July 13, 2021. https://emergency.cdc.gov/cerc/ppt/CERC_Crisis_Communication_Plans.pdf.

Cybersecurity and Infrastructure Security Agency. *Active Shooter Emergency Action Plan Guide and Template*. Accessed July 13, 2021. https://www.cisa.gov/publication/active-shooter-emergency-action-plan-guide.

Cybersecurity and Infrastructure Security Agency. Active Shooter Preparedness Webpage. Accessed July 13, 2021. https://www.cisa.gov/active-shooter-preparedness.

Cybersecurity and Infrastructure Security Agency. Critical Infrastructure Exercises Webpage. Accessed July 13, 2021. https://www.cisa.gov/critical-infrastructure-exercises.

Cybersecurity and Infrastructure Security Agency. *Cyber Essentials Toolkits*, 2020. Accessed July 13, 2021. https://www.cisa.gov/publication/cyber-essentials-toolkits.

Cybersecurity and Infrastructure Security Agency. Dams Sector Resources Webpage. Accessed July 13, 2021. https://www.cisa.gov/dams-sector-resources.

Cybersecurity and Infrastructure Security Agency. Industrial Control Systems Recommended Practices Webpage. Accessed July 13, 2021. https://us-cert.cisa.gov/ics/Recommended-Practices.

Cybersecurity and Infrastructure Security Agency. *Recommended Practice: Industrial Control Systems Cyber Security Incident Response Capability*, October 2009. Accessed July 13, 2021. https://us-cert.cisa.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf.

Cybersecurity and Infrastructure Security Agency. What To Do – Bomb Threat Website. Accessed July 13, 2021. https://www.cisa.gov/what-to-do-bomb-threat.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. *Bomb Threat Checklist*. Accessed July 13, 2021. https://tripwire.dhs.gov/documents/dhs-bomb-threat-checklist.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. Training Video Series Webpage. Accessed July 13, 2021. https://tripwire.dhs.gov/training-video-series.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. Virtual Instructor-Led Training Webpage. Accessed July 13, 2021. https://tripwire.dhs.gov/training/381.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. Web-Based Independent Study Training Webpage. Accessed July 13, 2021. https://tripwire.dhs.gov/training/376.

Cybersecurity and Infrastructure Security Agency, Office for Bombing Prevention. *VBIED Identification Card*. Accessed July 13, 2021. https://tripwire.dhs.gov/documents/vbied-identification-card.

Defense Security Cooperation Agency. *Incident Response Plan Template*, February 2020. Accessed July 13, 2021. https://www.dcsa.mil/Portals/91/Documents/CTP/tools/Incident_Response_Plan_Template_(February2020).pdf.

Environmental Protection Agency. Develop and Conduct a Water Resilience Tabletop Exercise with Water Utilities Webpage. Accessed July 13, 2021. https://www.epa.gov/waterresiliencetraining/develop-and-conduct-water-resilience-tabletop-exercise-water-utilities.

Environmental Protection Agency, Water Resilience. America's Water Infrastructure Act: Risk Assessments and Emergency Response Plans Webpage. Accessed July 13, 2021. https://www.epa.gov/waterresilience/awia-section-2013#ERP.

Federal Bureau of Investigation. Crisis Communications Quick Reference Guide. Accessed July 13, 2021. https://www.dhs.gov/sites/default/files/publications/fbi-crisis-communications-trifold-reference-guide.pdf.

Federal Bureau of Investigation. *Developing Emergency Operations Plans: A Guide for Businesses*, 2018. Accessed July 13, 2021. https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf.

Federal Emergency Management Agency. *Comprehensive Preparedness Guide 101: Developing and Maintaining Emergency Operations Plans*, November 2010. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-07/developing-maintaining-emergency-operations-plans.pdf.

Federal Emergency Management Agency. *Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review Guide, 3rd Edition*, May 2018. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-07/threat-hazard-identification-risk-assessment-stakeholder-preparedness-review-guide.pdf.

Federal Emergency Management Agency. *Continuity of Operations: An Overview*. Accessed July 13, 2021. https://www.fema.gov/pdf/about/org/ncp/coop_brochure.pdf.

Federal Emergency Management Agency. *Emergency Action Plans for Dam Owners Fact Sheet.* Accessed July 13, 2021. https://damsafety.org/sites/default/files/FactSheet_EAP_0.pdf.

Federal Emergency Management Agency. *Emergency Action Planning for State Regulated High Hazard Potential Dams (FEMA 608)*, August 2007. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-08/fema608.pdf.

Federal Emergency Management Agency. *Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements*, January 2017. Accessed July 13, 2021. https://www.gpo.gov/docs/default-source/accessibility-privacy-coop-files/January2017FCD1-2.pdf.

Federal Emergency Management Agency. *Federal Continuity: National Continuity Programs Brochure*, July 2018. July 13, 2021. https://www.fema.gov/sites/default/files/2020-07/fema_brochure-continuity-ncp_082318_0.pdf.

Federal Emergency Management Agency. *Federal Guidelines for Dam Safety (FEMA P-93)*, April 2004. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-08/fema_dam-safety_P-93.pdf.

Federal Emergency Management Agency. *Federal Guidelines for Dam Safety: Emergency Action Planning for Dam Owners (FEMA 64)*, July 2013. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-08/eap_federal_guidelines_fema_p-64.pdf.

Federal Emergency Management Agency. *Federal Guidelines for Dam Safety Risk Management (FEMA P-1025)*, January 2015. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-08/fema_dam-safety_risk-management_P-1025.pdf.

Federal Emergency Management Agency. *Federal Guidelines for Inundation Mapping of Flood Risks Associated with Dam Incidents and Failures (FEMA P-946)*, July 2013. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-08/fema_p-946_dam_guidance.pdf.

Federal Emergency Management Agency. Homeland Security Exercise and Evaluation Program (HSEEP) Webpage. Accessed July 13, 2021. https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep#.

Federal Emergency Management Agency. ICS Resource Center Webpage. Accessed July 13, 2021. https://training.fema.gov/emiweb/is/icsresource/icsforms/.

Federal Emergency Management Agency. National Dam Safety Program Publications Webpage. Accessed July 13, 2021. https://www.fema.gov/emergency-managers/risk-management/dam-safety/publications.

Federal Emergency Management Agency. National Incident Management System (NIMS) Webpage. Accessed July 13, 2021. https://www.fema.gov/emergency-managers/nims.

Federal Emergency Management Agency. *National Response Framework, 4th Edition*, October 2019. Accessed July 13, 2021. https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf.

Federal Emergency Management Agency. *Risk Communication for Dams Fact Sheet*. Accessed July 13, 2021. https://damsafety.org/sites/default/files/FactSheets_RiskComm_v2_0.pdf.

Federal Energy Regulatory Commission. Emergency Action Plan (EAP) Program Webpage, June 2020. Accessed July 13, 2021. https://www.ferc.gov/emergency-action-plan-eap-program.

Federal Energy Regulatory Commission. *Engineering Guidelines for the Evaluation of Hydropower Projects, Chapter 6 Emergency Action Plans,* July 2015. Accessed July 13, 2021. https://www.ferc.gov/sites/default/files/2020-04/chap6.pdf.

Federal Energy Regulatory Commission. Potential Failure Mode Analysis Webpage, July 2020. Accessed July 13, 2021. https://www.ferc.gov/industries-data/hydropower/dam-safety-and-inspections/dspmppfma-potential-failure-mode-analysis.

Federal Energy Regulatory Commission. *Preparations for Handling Emergencies and Potential Emergencies at Projects*, May 2005. Accessed July 13, 2021. https://www.ferc.gov/sites/default/files/2020-04/prep.pdf.

Federal Energy Regulatory Commission. *Risk-Informed Decision-Making Risk Guidelines for Dam Safety*, March 2016. Accessed July 13, 2021. https://www.ferc.gov/industries-data/hydropower/dam-safety-and-inspections/risk-informed-decision-making-ridm-3.

Federal Energy Regulatory Commission. *Security Program for Hydropower Projects Revision 3—Dam Assessment Matrix for Security and Vulnerability Risk (DAMSVR)*, June 2009. Accessed July 13, 2021. https://www.ferc.gov/industries-data/hydropower/dam-safety-and-inspections/security-program-hydropower-projects-0.

Federal Energy Regulatory Commission, Division of Dam Safety and Inspections. *FERC Security Program for Hydropower Projects Revision 3A*, March 2016. Accessed July 13, 2021. https://www.ferc.gov/sites/default/files/2020-04/security.pdf.

Federal Energy Regulatory Commission, North American Electric Reliability Corporation, and Regional Entities. *Cyber Planning for Response and Recovery Study (CYPRES),* September 2020. Accessed July 13, 2021. https://cms.ferc.gov/sites/default/files/2020-09/FERC%26NERC_CYPRES_Report.pdf.

Interagency Security Committee. *Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide*, 2021. Accessed July 13, 2021. www.cisa.gov/publication/planning-and-response-active-shooter-interagency-security-committee-policy-and-best.

*International Standards Organization (ISO). *ISO 2301: Security and Resilience—Business Continuity Management Systems*, October 2019. Accessed July 13, 2021. https://www.iso.org/standard/75106.html.

MITRE Corporation. ATT&CK® for Industrial Control Systems Webpage, March 2020. Accessed July 13, 2021. https://collaborate.mitre.org/attackics/index.php/Main_Page.

National Academies and the U.S. Department of Homeland Security. *IED Attack: Improvised Explosive Devices Fact Sheet*. Accessed July 13, 2021. https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf.

National Association of Secretaries of State. *Issue Briefing: Planning for Cyber Incident Response*, February 2020. Accessed July 13, 2021. https://www.nass.org/sites/default/files/Cybersecurity/IRP_Issue_Briefing_02.11.20.pdf.

*National Fire Protection Association. *NFPA 1600: Standard on Continuity, Emergency, and Crisis Management*, 2019. Accessed July 13, 2021. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600.

National Institute of Standards and Technology (NIST) *Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide Recommendations*, August 2012. Accessed July 13, 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

National Institutes of Science and Technology, Information Technology Laboratory. Small Business Cybersecurity Corner Webpage. Accessed July 13, 2021. https://www.nist.gov/itl/smallbusinesscyber.

New Jersey Department of Environmental Protection, Bureau of Dam Safety and Flood Control. *Guidelines for Developing and Emergency Action Plan*, March 2011. Accessed July 13, 2021. www.nj.gov/dep/damsafety/docs/eapform.pdf.

North American Electric Reliability Corporation. CIP Reliability Standards Webpage. Accessed July 13, 2021. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

North American Electric Reliability Corporation. *Cyber Security–Incident Reporting and Response Planning, Implementation Guidance for CIP-008-6*, January 2019. Accessed July 13, 2021. https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/Implementation_Guidance_for_CIP-008-6_Final_Ballot_01152019.pdf.

Ready.gov. Crisis Communication Plan Webpage. Accessed July 13, 2021. https://www.ready.gov/crisis-communications-plan.

Sandia National Laboratory, News Release. "Two new methodologies can help owners improve security of nation's dams and power systems", December 10,2001. Accessed July 13, 2021. https://www.sandia.gov/media/NewsRel/NR2001/ramdramt.htm.

U.S. Department of Agriculture, Natural Resources Conservation Service. Emergency Action Plans (EAPs) Webpage. Accessed July 13, 2021. https://www.nrcs.usda.gov/wps/portal/nrcs/detail/national/ndcsmc/?cid=nrcs143_009164.

U.S. Department of Homeland Security. *Dams Sector: Estimating Loss of Life for Dam Failure Scenarios*, September 2011. Available on the HSIN-CI Dams Portal.

U.S. Department of Homeland Security. *Homeland Security Presidential Directive (HSPD)-5, Management of Domestic Incidents*, February 2003. Accessed July 13, 2021. https://www.dhs.gov/publication/homeland-security-presidential-directive-5.

U.S. Department of Homeland Security. *Presidential Policy Directive 8, National Preparedness*, March 2011. Accessed July 13, 2021. https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

U.S. Department of Homeland Security, Buildings and Infrastructure Protection Series. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA-426/BIPS-06),* October 2011. Accessed July 13, 2021. https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf.

U.S. Department of Homeland Security, U. S. Department of Justice. *DHS-DOJ Bomb Threat Guidance*. Accessed July 13, 2021. https://www.cisa.gov/sites/default/files/publications/Bomb-Threat-Guidance-Quad-Fold.pdf.

U.S. Department of Homeland Security, U. S. Department of Justice. *Bomb Threat Standoff Card*. Accessed July 13, 2021. https://tripwire.dhs.gov/documents/dhs-doj-bomb-threat-stand-card.

U.S. Department of Homeland Security, U. S. Department of Justice. *Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance*, 2017. Accessed July 13, 2021. https://www.cisa.gov/sites/default/files/publications/Security-and-Resiliency-Guide-Counter-IED_0.pdf.

U.S. Department of Homeland Security, U. S. Department of Justice. *Unattended vs. Suspicious Activity Card*, December 2019. Accessed July 13, 2021. https://tripwire.dhs.gov/documents/unattended-vs-suspicious-items-card.

U.S. Department of the Interior, Bureau of Reclamation. *Guidelines for Estimating Life Loss for Dam Safety Risk Analysis*, July 2015. Accessed July 13, 2021. https://www.usbr.gov/ssle/damsafety/documents/RCEM-Methodology2015.pdf.

U.S. Department of Justice, Cybersecurity Unit. *Best Practices for Victim Response and Reporting of Cyber Incidents*, September 2018. Accessed July 13, 2021. https://www.justice.gov/criminal-ccips/file/1096971/download.