Dams Sector Security Guidelines

2015

Homeland Security

Acknowledgments

This document was developed with input, advice, and assistance from the Dams Sector Security Education Working Group (SEWG) and council members of the Dams Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC), which included representatives from the public and private sector.

The "Dams Sector Security Guidelines" consolidates effective industry security practices into a voluntary framework for owners and operators to select and implement security activities and measures that promote the protection of personnel, public health, public safety, and public confidence. The document is intended as a valuable resource to small- and medium-sized owners and operators, including security directors and facility managers with varying levels of security knowledge.

Contents

Executive Summary

The Dams Sector encompasses dam projects, power plants, navigation locks, levees, mine tailings, industrial waste impoundments, dikes, hurricane barriers, and other similar water retention and water control facilities throughout the Nation. Distinguishing characteristics of the sector include the diversity of owners, operators, and regulators and the wide range of sector assets in terms of size, function, and criticality. Assets range from large hydroelectric dams, coastal levee systems, and water supply reservoirs that support and protect whole regions to small, locally owned dams and levees that serve individual agricultural areas. In addition, dam projects are complex facilities that may include assets such as multiple water impoundment or control structures, reservoirs, spillways, outlet works, powerhouses, and canals or aqueducts. Regardless of their size, dams and levees provide a wide range of economic, environmental, and social benefits.

Risks to physical and cyber assets originate from multiple sources, including deliberate, malicious human actions (e.g., crime and terrorism); non-malicious human actions (e.g., accidents, negligence); structural and technological deficiencies; and natural disasters. Complete or partial failure of critical dams, locks, and levees could result in catastrophic downstream flooding, loss of life, and significant direct and indirect economic impacts, making these assets potentially attractive targets. Each owner or operator manages unique assets; a distinct risk profile; and tailored operational processes, business environments, and security practices.

Risks to the Dams Sector

- Theft and vandalism
- Accidents
- Aging infrastructure
- Structural deficiencies
- Natural disasters
- Attacks on physical or cyber infrastructure

The overall security level of individual assets evolves over time and varies in accordance with site-specific conditions and threats. Owners and operators must identify critical assets on which to focus additional security reviews, determine the level of risk that is practical and acceptable for their assets at a particular point in time, and implement security practices appropriate to the level of risk and resources available. The wide range of sector security practices includes research and development efforts, multi-jurisdictional regional exercises, comprehensive training and outreach initiatives, and implementation of plans to support incident response and restoration. These practices are often guided or directed by requirements associated with Federal and State laws, regulations, and authorities. Despite variances in regulatory control, specific security practices can aid any Dams Sector owner or operator with identifying, understanding, and mitigating risk to assets, systems, and networks.

Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

– Presidential Policy Directive 21

The "Dams Sector Security Guidelines" consolidate effective industry security practices into a framework for owners and operators to select and implement security activities and measures that promote the protection of personnel, public health, public safety, and public confidence. Owners and operators may review the document in full, or focus their review on specific security practice components that address their security needs or augment existing security practices. For additional information about the Dams Sector composition, risk profile, and risk management activities, refer to the "Dams Sector-Specific Plan" located at http://www.dhs.gov/dams-sector.

Security Practices

On a daily basis, owners and operators take actions that support risk management planning and investments in security as necessary components of prudent business planning and operations. The security practices of each owner and operator—which range from select risk management activities and measures to enacting and monitoring a formal security program—

help increase organizational safety and security, safeguard personnel, and prevent unauthorized access to assets, business processes, control systems, equipment, and sensitive information. By applying the basic security fundamentals and industry effective practices, owners and operators can identify and implement security measures consistent with the criticality of the site and business processes and appropriate for the level of acceptable risk for each facility selected for enhanced security.

For many owners and operators, the level of security investments reflects risk-versus-consequence tradeoffs that are based on two factors: what is known about the risk environment and what is economically justifiable and sustainable in a competitive marketplace or within resource constraints. Further, security enhancement investments often compete with other investments, with many decision-makers finding it difficult to justify security expenditures without a strong business case. By systematically leveraging industry effective practices, such as those identified in the Guidelines, owners and operators can target security investments for specific assets based on assessed risk and associated security measures to reduce risk. Benefits may include satisfying safety and security regulatory requirements, improving brand image, increasing preparedness, reducing impacts and frequency of disruptions, and realizing cost efficiencies through streamlining and integrating security processes.

Identifying critical assets represents the first step in systematically increasing security by applying targeted security measures. Many tools are available to aid owners and operators in identifying and then prioritizing critical assets, largely based on whether assets in their portfolio are federally regulated. Chapter 1 provides additional information about these tools. The implementation of security practices, including assessments and security measures, follows the identification and prioritization of assets. Dams Sector security practices are commonly divided into four categories (as depicted in Figure 1): physical, cyber, personnel, and information. The following briefly summarizes these practices, with additional information on the various tools, capabilities, and templates available to owners and operators found in Chapters 2–5.

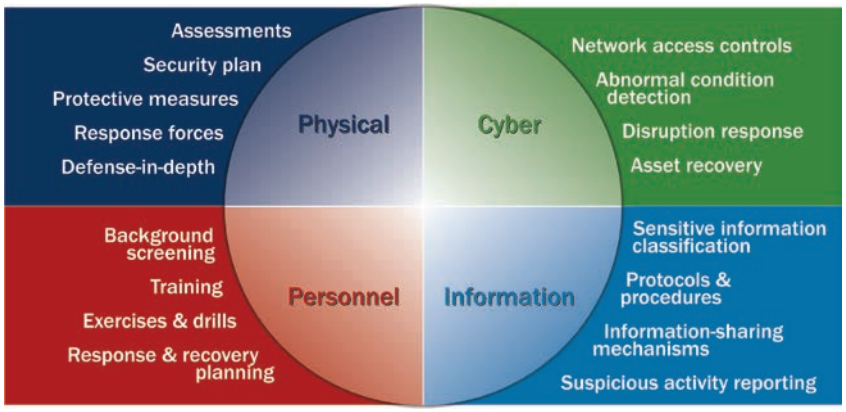


Figure 1. Sample security practice components

Physical Security Practices: Security risk assessments that feature threat, vulnerability, and consequence components can help owners and operators make cost-effective risk mitigation investments across their portfolio. Owners and operators may choose to conduct an individual assessment to understand a specific component or implement a full, comprehensive security risk assessment to take into account all three individual components. A variety of physical security measures could then be selected to mitigate risk. Generally designed and installed to perform the specific functions in relation to an attack or disruption of an asset (e.g., prevent or deter, detect and assess, delay and deny, respond, and restore), owners and operators may choose to implement particular physical security measures to improve those functions or implement a comprehensive approach to integrate multiple functions.

Cybersecurity Practices: Security in the Dams Sector is not limited to only the physical environment, but also encompasses the ever-evolving cyber environment. Achieving security and resilience in cyberspace begins with identifying and assessing critical cyber assets and systems, as well as the cyber risks and vulnerabilities to the facility and connecting networks. Deficient cybersecurity functions can then be selected for further analysis. Once the cyber landscape has been understood, the owner or operator is then able to implement targeted cybersecurity practices to improve the cybersecurity posture and address the risks and vulnerabilities uncovered. In implementing cybersecurity practices, owners and operators may choose to implement practices to address select deficiencies. However, given the evolving cyber landscape and myriad unknowns, owners and operators may best improve their cybersecurity posture through persistent implementation of comprehensive cybersecurity risk management: identify, protect, detect, respond, and recover.

Personnel Security Practices: Owners, operators, personnel, and contractors all perform mission-critical tasks to operate assets, systems, and networks and implement security measures. The errant or illicit actions of one person can cause catastrophic damage to facilities, surrounding communities, and the environment. Assessing threats includes conducting background screening for potential and new hires or contractors, periodic re-screening of existing personnel, and determining the likelihood of, and vulnerability to, insider threats. Personnel security measures include background investigations, training to increase security awareness and education, exercises and drills to hone skills and knowledge related to specific types of security incidents, and the development and management of response and recovery plans.

Information Security Practices: Securing information is a critical component of robust security practices. Without appropriate information security measures, vulnerabilities can be exploited to cause harm or disrupt facility functions. In developing information security practices, information assets are first identified, and the landscape in which these assets reside is documented. This information is then used to conduct a risk assessment, with the results of the assessment enabling the owner or operator to implement information security measures in an informed manner. Critical information security measures include identification and protection functions; however, the security measures referenced herein under *Physical Security Practices* and *Cybersecurity Practices* can be leveraged to secure physical information and electronic information, respectively.

How to Use the "Dams Sector Security Guidelines"

The "Dams Sector Security Guidelines" consolidates effective industry security practices into a framework to help owners and operators select and implement security activities and measures that reduce risk; improve the protection of personnel, public health, and public safety; and reinforce public confidence.

Specifically, the "Dams Sector Security Guidelines" outline various strategies and methods to help select and implement security activities and measures appropriate to a facility. Each section of the document focuses on a distinct aspect of sector security practices—physical, cyber, personnel, and information—and includes industry-recognized effective practices and means by which to obtain additional information. Links to all documents referenced herein are located in *Appendix H: Source Documents and Websites*.

Owners and operators are encouraged to review the information contained in the "Dams Sector Security Guidelines" and implement the security practices appropriate for the facility's risk profile, operational processes, business environments, regulatory requirements, and available resources. It is important to note that, though this document separates the security topics into different chapters, many of the practices are inextricably linked. For example, many critical physical assets are controlled, operated, and maintained through cyber infrastructure. Further, all physical, cyber, and personnel security measures rely on adequate information security measures to be effective. As such, users of the "Dams Sector Security Guidelines" need not proceed sequentially through the chapters and may instead select the sections of most interest.

Disclaimer

The information provided in the "Dams Sector Security Guidelines" is not intended to supersede, modify, or replace any existing laws, regulations, codes, standards, or policies applicable to the sector. The publication of "Dams Sector Security Guidelines" does not constitute endorsement of any product or product type, nor does it test, certify, or approve any products. The use of this document is entirely voluntary. The "Dams Sector Security Guidelines" recognizes that the overall level of security will vary in accordance with site-specific conditions and specific threats to each individual asset. Each owner and operator must decide the level of risk that it is considered practical and acceptable, as well as the corresponding security practices.

1. Critical Asset Identification

Critical assets are defined as those facilities whose destruction or compromise would result in a high-consequence event—significant long-term negative consequences, such as loss of life, adverse public health and safety, economic hardship, or a damaging psychological effect on our Nation. Identifying and protecting critical assets is the foundation of any security program and provides the starting point from which sector owners and operators may apply effective measures for the physical, cyber, personnel, and/or information security of those assets. By identifying and prioritizing critical assets, owners and operators can better mitigate the impact of worst-case scenarios and prepare for high-profile incidents.

Many tools are available to help sector owners and operators identify critical assets. Figure 2 represents options from which owners and operators may choose for critical asset identification, organized by whether assets within the owner's or operator's portfolio are regulated. Depending on the portfolio, some facilities may fall under more than one regulatory authority, or may choose to voluntarily implement guidelines if they are not regulated. Example options include:

- **Regulated:** If portions of the infrastructure portfolio are federally regulated, those assets are often categorized for criticality by the Federal Energy Regulatory Commission (FERC) Division of Dam Safety and Inspections through specific criteria and processes. For medium-to-large-scale facilities and projects, the FERC Office of Electric Reliability, through the North American Electric Reliability Corporation (NERC), determines and also requires compliance with Critical Infrastructure Protection (CIP) standards. Smaller facilities and projects may not be subject to NERC regulation.
- **Self-Regulated:** Federal agencies with self-governing regulatory authorities identify, protect, and prioritize assets based on their own criteria of criticality relative to what is most important to the agency or business mission. The "Risk Management Process for Federal Facilities: An Interagency Security Committee Standard" provides additional information on the criteria and processes for determining facility security levels for all Federal facilities.
- **Not Regulated:** For assets that are not regulated, owners and operators can identify criticality based on their own criteria, or follow the relevant existing regulatory requirements and/or voluntary guidelines that define asset criticality and associated identification methodology. Though such assets are not regulated, owners and operators may choose to follow the relevant guidelines as effective standard business practices for critical asset identification and prioritization.

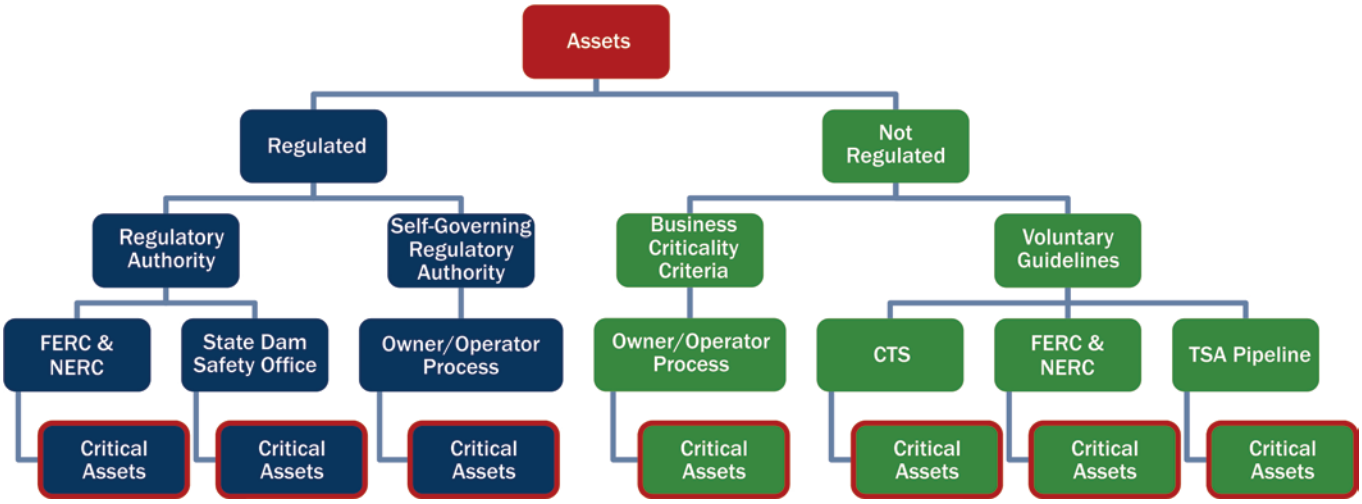


Figure 2. Options for identifying critical assets, based on whether the asset is regulated

Common guidelines by which, as appropriate, sector owners and operators may identify and prioritize their portfolio of critical assets include:

- Dams Sector Consequence-Based Top Screen (CTS) Methodology
- FERC Division of Dam Safety and Inspections "Security Program for Hydropower Projects" (Revision 3)
- NERC "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets"
- U. S. Department of Homeland Security (DHS) Transportation Security Administration (TSA) "Pipeline Security Guidelines"

In addition to Federal regulation, many sector assets are also regulated at the State level, though largely for State dam safety laws rather than dam security. However, some State safety regulations, including requirements for emergency action plans (EAPs), may relate to security as well (see *Chapter 4: Personnel Security Practices* for more information on EAPs). For specific information on State regulation of sector assets, owners and operators can contact their State dam safety official. A listing of contact information for State dam safety officials is available from the Association of State Dam Safety Officials Website (http://www.damsafety.org/map/). In addition, State homeland security agencies may be a resource for listings of State-level critical assets, as identified through the DHS National Critical Infrastructure Prioritization Program.

Consequence-Based Top Screen Methodology

For sector owners and operators with multiple facilities to assess, the CTS methodology can assist in identifying and prioritizing critical assets. The purpose of the CTS methodology is to identify critical assets within the Dams Sector at the portfolio level (e.g., owner, State, regional, and national). By focusing on potential consequences and decoupling the analysis from the threat and vulnerability components of the risk process, the CTS approach can serve as an effective all-hazards preliminary prioritization scheme.

For more information on the Consequence-Based Top Screen (CTS) methodology, contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

By using metrics that cover a range or spectrum of potential values, the CTS screening methodology is completely scalable and can be effectively implemented at different portfolio levels. Therefore, the CTS process could assist in identifying assets that may be of regional or State significance by adopting consequence thresholds that are appropriate for each case.

When screening and prioritizing using the CTS methodology, four parameters are assessed for potential impacts associated with severe damage or disruption to the asset:

- **Human Impacts:** The impacts on human health and safety caused by inundation of downstream populated areas, industrial areas, and other critical infrastructure assets;
- **Economic Impacts:** The impacts associated with damages to the asset, direct damage to downstream inundated areas, and direct monetary impacts associated with lost project benefits;
- **Impacts on Critical Functions:** The secondary effects associated with the disruption or loss of the critical functions provided by the asset; and
- **National or State-Level Impacts:** A standard set of cross-sector impacts used to identify assets of national or State significance in terms of potential consequences.

The prioritization information obtained from the CTS process can support decisions regarding the need for additional analyses and detailed studies. For example, in the case of an owner responsible for a large portfolio of dams, those facilities identified as critical assets through the CTS process could be assigned higher priority for conducting detailed risk assessments. The results from the CTS process could also effectively inform decision-makers about assets within a specific area that should receive particular attention from the emergency management community because of their potential for significant impacts.

FERC "Security Program for Hydropower Projects"

As part of security program and measures guidance, the FERC "Security Program for Hydropower Projects" describes three security groups (Security Groups 1, 2, and 3) for dams. The FERC Division of Dam Safety and Inspections determines the criticality of sector assets through the division's own protected criteria and methodology, the Dam Assessment Matrix for Security and Vulnerability Risk (DAMSVR). FERC notifies sector owners and operators of the Security Group determination of their facilities, which are placed into Security Group 1, 2, or 3 based on risk criteria using Consequence (C), Vulnerability (V), and Likelihood of Attack (L) values of the DAMSVR analysis. This determination delineates the different security regulatory requirements for those facilities based on their Security Group designation.

Resources for Additional Information

- "Dams Sector Security Guidelines" (Chapter 3: Cybersecurity Practices)
- FERC Dam Assessment Matrix for Security and Vulnerability Risk
- FERC "Security Program for Hydropower Projects" (Section 9.2: Critical Cyber Asset Identification)

The FERC "Security Program for Hydropower Projects" document provides guidelines for identifying critical cyber assets based on criteria relating to two potential consequences: (1) the unintentional release of all or part of the reservoir affecting the downstream population and infrastructure and (2) non-operation of a licensed facility resulting in a loss of significant power generation. A cyber asset's criticality is based on the exceedance of FERC-specified consequence threshold values, and will determine the level of security measures (baseline or enhanced) to be implemented. *Appendix E* of this document provides information on these cybersecurity measures. Each facility follows a flowchart of action to determine whether the critical cyber asset guidelines apply to that facility. Projects with critical cyber assets must ensure their interconnected facilities (e.g., Security Group 3 dams) meet the same cybersecurity measures. Projects without remote or automated controls—the first determination in whether the requirements apply—are not required by FERC to implement cybersecurity measures, but must annually reassess criticality of cyber assets. However, some owners and operators may voluntarily choose to follow the requirements in the interest of business continuity.

NERC "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets"

The NERC "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets" provides a methodology to identify cyber assets that are essential to the reliability or operability of the facilities and control systems necessary for operating an interconnected electric energy transmission network. For the Dams Sector, this is directly relevant to hydropower facilities and assets, yet the NERC guideline may also be relevant and beneficial for other portions of the sector. For example, the NERC guideline provides a basis for identifying critical cyber assets relating to control systems, which are common and important assets throughout the sector. The NERC "Cyber Security – Critical Cyber Asset Identification Standard" describes the identification and documentation of the critical cyber assets (e.g., master and remote monitoring and control systems, including backup systems) associated with the overall critical assets that support the reliable operation of the electric energy transmission network.

Resources for Additional Information

- "Dams Sector Security Guidelines" (Chapter 3: Cybersecurity Practices)
- NERC "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets"
- NERC "Cyber Security – Critical Cyber Asset Identification Standard" (document undergoing an update in 2015)

To assist owners and operators in identifying critical cyber assets, the NERC guideline helps to define what assets should be evaluated, provides risk-based evaluation guidance for determining critical cyber assets, and describes reasonable bases to support that determination. The process of identifying critical cyber assets in the NERC guideline consists of five steps:

- **Identify cyber assets:** Define cyber assets associated with a critical asset;
- **Group cyber assets:** Organize cyber assets by application;
- **Determine essential cyber assets:** Assess the cyber assets to identify those that support one or more essential functions of a critical asset;

- **Identify cyber assets with qualifying connectivity:** Apply connectivity requirements to further narrow the list of essential cyber assets; and
- **Compile critical cyber assets:** Document the final list of critical cyber assets.

The identification process and subsequent evaluations are intended to be performed in consultation with system operators and planning engineers using system studies, analyses, simulations, and/or historical experience.

TSA "Pipeline Security Guidelines"

The DHS TSA "Pipeline Security Guidelines" provide a simplified process to determine facility and asset criticality, which may be more appropriate for owners and operators without an extensive, multisite portfolio of assets. Though "Pipeline Security Guidelines" is intended for use by natural gas and hazardous liquid pipeline facility owners and operators, the methodology for identifying critical assets is readily applicable to Dams Sector projects, sites, and assets. Owners and operators are encouraged to determine facility criticality based on criteria indicating the severity of potential impacts resulting from that facility's damage or destruction. A facility is considered critical if its damage or destruction would have the potential to do one or more of the following:

Resources for Additional Information

- "Dams Sector Security Guidelines" (Appendix B: TSA Criticality Determination Pathway)
- TSA "Pipeline Security Guidelines" (Section 5: Criticality)

- Disrupt or significantly reduce required service or deliverability to installations identified as critical to national defense;
- Disrupt or significantly reduce required service or deliverability to other critical infrastructure, resulting in major economic disruption;
- Cause mass casualties or significant detrimental health effects;
- Disrupt or significantly reduce a State or local government's ability to provide essential public services and emergency response for an extended period of time;
- Significantly damage or destroy national landmarks or monuments;
- Disrupt or significantly reduce the intended usage of major rivers, lakes, or waterways (e.g., public drinking water for large populations or major commerce or public transportation routes);
- Disrupt or significantly reduce required service or deliverability to a significant number of customers or individuals for an extended period of time; and
- Significantly disrupt facility operations (e.g., business critical facilities) for an extended period of time.

Sector owners and operators may choose to use the TSA "Pipeline Security Guidelines" methodology to first determine facility criticality and subsequently follow the same criteria to determine critical assets within those facilities identified as critical.

2. Physical Security Practices

The cornerstone of maintaining dam security and resilience is the collective array of physical security practices that protect and secure critical assets. Identifying critical assets provides the starting point for an integrated approach to physical protection, with owners and operators utilizing a variety of methods to identify and prioritize assets (as discussed in Chapter 1: Critical Asset Identification). Following the identification of critical assets, subsequent security risk assessments that feature threat, vulnerability, and consequence components can help owners and operators make cost-effective risk mitigation investments across their portfolio.

Owners and operators may then choose to implement physical security measures for mitigating risk in different ways, according to the defining characteristics and operating environment (including regulatory requirements) of their portfolio. Options range from adopting or expanding distinct security measures (e.g., surveillance, access control, and barrier systems) to developing and administering a comprehensive physical security plan. Owners and operators can choose to conduct the level of risk assessment that is most appropriate to their objectives. This may entail conducting a full, comprehensive risk assessment or an individual consequence, vulnerability, or threat assessment for an express purpose.

Conduct Physical Risk Assessments

A thorough and complete risk assessment is a common industry approach by which to define appropriate physical security practices. Risk is understood as the probability of an undesirable event occurring, or the capacity for a potential loss and its probability of occurrence. Assessing risk entails identifying the undesired event (or consequence) and the probability of its occurrence, which includes examining threat and vulnerability. While assessment methodologies may vary in scope, the foundational understanding of risk remains the same.

Risk = Consequence x Vulnerability x Threat

Figure 3. Equation for calculating risk. Risk is calculated as a function of consequence, vulnerability, and threat.

Physical security is assessed through a risk-based process in which risk is assessed as a function of threats, vulnerabilities, and consequences. Although these risk components are standard, the wide variation of assets within the Dams Sector motivates sector partners to use a range of individual threat, vulnerability, or consequence assessment methodologies and/or comprehensive risk assessment methodologies.

Most security risk assessments are informed by all of the individual types of assessment—threat, vulnerability, and consequence. However, an owner or operator may choose to conduct an individual risk assessment to understand a specific security component of the facility or asset. The risk assessment conducted is only as good as the accuracy of the variables entered into the equation. Calculating absolute risk—based on specific standard units of risk measurements—may be challenging based on limited or imperfect information. Instead, the owner or operator may find it more meaningful and manageable to calculate relative risk based on measuring risk as a ratio. In calculating relative risk, the owner or operator compares the risk value of the scenario relative to other similarly constructed risk values. In addition, utilizing relative risk avoids the disclosure of sensitive information, but still conveys to decision-makers the significance of the risk.

Resources for Additional Information

- "Dams Sector Protective Measures Handbook" (FOUO) (Section 6: Risk Management and Assessment)
- DHS Risk Lexicon

Consequence Assessment

Consequence is measured as the range of loss or damage resulting from an undesired event. The determination of the consequences of an attack on a critical asset must consider both catastrophic events that result in total failure and attacks that result in the asset operating at a reduced capacity. A full consequence assessment takes into consideration specific public health and safety, economic, psychological, and governmental impacts. However, estimating potential indirect impacts downstream requires assumptions and complex variables. The four main categories of consequence include:

Resources for Additional Information

- "Dams Sector-Specific Plan"
- Dams Sector "Estimating Loss of Life for Dams Failure Scenarios"
- Dams Sector "Estimating Economic Consequences for Dam Failure Scenarios"

- **Public Health and Safety**: Effects on human life and physical well-being (e.g., fatalities, injuries);
- **Economic**: Direct and indirect effects on the economy (e.g., costs to rebuild the asset, costs to respond to and recover from an attack);
- **Psychological**: Effects on public morale and confidence in national economic and political institutions; and
- **Governance/Mission Impact**: Effects on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

At a minimum, consequence assessments focus on two fundamental impacts: human (loss of life) and direct economic impacts. Both of these fundamental impacts can be referenced during the initial asset identification process to help determine whether an asset is defined as a critical asset. If multiple critical assets are present, then each asset may be evaluated separately for consequences. Once the consequence of each critical asset disruption has been established, the owner or operator can rank each asset by its criticality and create a prioritized list of critical assets. The fundamental impacts for a minimum consequence assessment include:

- **Loss of Life:** The expected number of fatalities from the event. Calculating loss of life requires an understanding of the total population at risk. This includes the total estimated number of people occupying residences, buildings, or recreational areas nearby, as well as the populations upstream/downstream of the dam that could be adversely affected by the loss.
- **Economic Impact:** The total economic losses that may occur. Calculating economic impact includes the estimation of lost project revenues, lost benefits during the disruption, costs to recover operations to full operating capacity, temporary and replacement costs of damaged or destroyed assets, total damages to downstream property, and environmental damage costs.

Vulnerability Assessment

Vulnerability is measured as the probability that an adversary would be successful in an attack and that the assets or components would be compromised. This includes assessing how easy the attack would be, how long it would take, and the probability of the adversary getting caught. Vulnerabilities include the design, location, security posture, process, or operation of an asset, system, or network that render it susceptible to destruction, incapacitation, or exploitation. A vulnerability assessment will identify areas of weakness that could result in undesired consequences and will take into account intrinsic structural weaknesses, protective measures, resilience, and redundancies. In trying to identify security vulnerabilities, potential aggressors may conduct sophisticated surveillance over a long period of time, which can be difficult to detect. The overall objective of surveillance activity is to determine possible targets, attack modes, and likelihood of success. Potential aggressors may seek to identify such features as presence or absence of security cameras, identification cards of personnel or contractors/vendors, or security event response types and timing.

Resources for Additional Information

- "Dams Sector Security Awareness Guide" (Objectives of Critical Infrastructure and Key Resources [CIKR] Surveillance)
- "Dams Sector Security Awareness Guide for Levees" (Objectives of CIKR Surveillance; Indicators of Possible Surveillance)
- U.S. Environmental Protection Agency (EPA) Vulnerability Self Assessment Tool
- DHS Risk Management for the Water Sector Training

Threat Assessment

Threats represent the probability of an attack by an adversary based on an analysis of motivation (intent) and capability. New or evolving threats to the continued reliability and integrity of infrastructure necessitate education and vigilance. The more the owner or operator knows about the actual and potential threats to its operations and mission, the more effective are the measures taken by the organization to protect critical assets. DHS has instituted the National Terrorism Advisory System (NTAS) to provide alerts on terrorist threats. In addition, owners should perform exercises to test and improve their security operations and plans prior to an actual threat level increase.

Resources for Additional Information

- "Dams Sector-Specific Plan"
- American Society of Civil Engineers (ASCE): "Guidelines for the Physical Security of Water Utilities and of Wastewater/ Stormwater Utilities" (Chapter 1.1.2: Design Basis Threat)
- National Terrorism Advisory System Website

The threat environment for the Dams Sector may be highly variable, but understanding common threat types will help the owner assess threats against its facilities and assets. Common threat types include vandalism, criminal, sabotage, insider, terrorist, or cyber.

Threat assessments analyze, evaluate, and quantify the threat variable of the risk equation. This includes examining not only what an adversary might be expected to do (i.e., the attack methodology), but also the likely tactics, techniques, procedures, weapons, or explosives used to carry out an attack. A threat assessment begins by identifying critical operations and assets within a facility. Threat assessments are a snapshot in time and may be performed periodically to ensure that the most up-to-date and available information is used during the assessment process. A threat assessment comprises three main areas:

- **Internal Threat Assessment:** Understanding one's own organization and personnel is key when protecting critical assets. The internal portion of a threat assessment commonly takes into account all of the staff, including personnel and contractors/vendors that have access to the facility and critical assets and operations. Developing an organization-wide program for deterring, detecting, and mitigating insider threats may include establishing an information-sharing process among human resources, intelligence, law enforcement, and other sources based on procedures compliant with all applicable laws and privacy requirements. A review of human resource and workforce relations actions and incident reports, provided by the human resources department or plant manager, can serve as a source for identifying personnel who may have malicious intent.
- **External Threat Assessment:** When performing the external portion of the threat assessment, it is advisable to involve local, State, and Federal law enforcement agencies. Such agencies can provide historical data and information on groups or individuals living or operating in the vicinity, and can keep owners and operators abreast of important changes in the threat environment. The Internet is another source for threat information. Information provided by these sources can augment information provided through a review of the facility's logs of security incidents and investigations.
- **Quantification and Application:** Once the internal and external threat information is acquired, it can be quantified and applied to the specific critical asset. By quantifying these areas, owners and operators can determine the likelihood of an attack and prioritize and plan for potential incidents, as well as implement appropriate security measures.

Comprehensive Security Risk Assessment

A security risk assessment is the comprehensive process of collecting information and assigning values to risks to make informed decisions pertaining to the management and mitigation of risk. The purpose of a security risk assessment is to identify critical assets and components, determine threats, and assess vulnerabilities and consequences continuously. A comprehensive security risk assessment will assist the decision-maker with making cost-effective investments in risk mitigation options to optimize expenditures and maximize performance of security countermeasures.

When performing a security risk assessment, an assessment team familiar with the type of dam and the components that are critical for the facility's operation can effectively understand disruption consequences. Once the vulnerability of the critical assets and components is assessed, an evaluation of the perceived threat can be applied to estimate the overall risk and to help establish a strategy for protection, response, and/or recovery. The risk assessment process is an ongoing process

and should be closely monitored, conducted periodically, and reassessed and modified as needed to protect critical assets. At a minimum, updates should be performed when site or threat conditions change.

Multiple security risk assessment methods are available to owners and operators, including the individual consequence, vulnerability, and threat assessments mentioned above. Risk assessment methodologies and tools that can be used to develop customized risk assessments for individual site needs include:

- Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) assessment methodology
- Risk Assessment Methodology for Dams (RAM-D)
- FERC Dam Assessment Matrix Security Vulnerability Risk (DAMSVR)
- Federal Emergency Management Agency (FEMA) Risk Prioritization Tool for Dams
- FERC Risk-Informed Decision Making (RIDM)
- U.S. Army Corps of Engineers (USACE) Common Risk Model for Dams (CRM-D) risk assessment methodology
- Environmental Protection Agency (EPA) Vulnerability Self Assessment Tool (VSAT) for Water and Wastewater Utilities

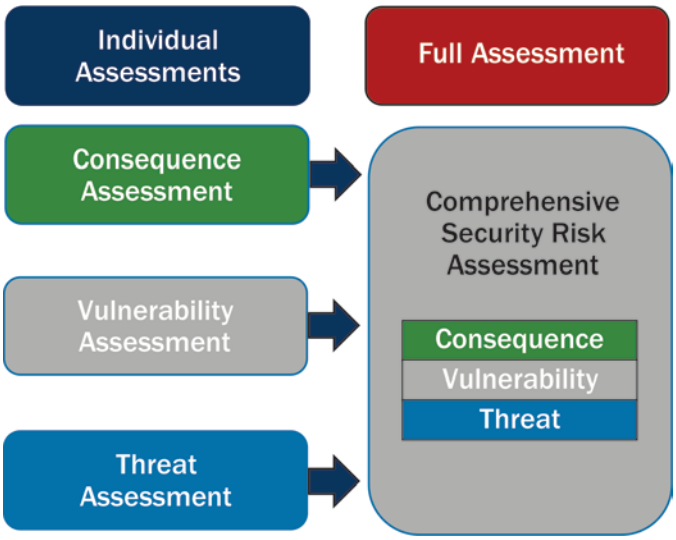


Figure 4. Individual assessment inputs into a comprehensive security risk assessment

Implement Physical Security Measures

Understanding consequences, vulnerabilities, threats, and overall risks for critical assets through assessments affords sector owners and operators the opportunity to select and implement physical security measures that may best address those risks. The basic principles of physical security are similar across many types of structures or components. The main differences for physical security among asset types are the degree of security required and the sophistication of layered protection needed to properly secure each asset.

When choosing physical security measures for critical assets, it is important to consider some fundamental concepts. Physical security measures are generally designed and installed to perform specific functions in relation to an attack or disruption of an asset: prevent or deter, detect and assess, delay and deny, respond, and restore. Depending on the results of assessments, regulatory requirements, and available resources, owners and operators may choose to implement particular physical security measures to improve those functions, or may adopt or expand on a comprehensive approach to implementing physical security measures. Whether specific or comprehensive, either path may include developing or adapting strategic plans for the facility or portfolio (such as a physical security plan or an EAP) to incorporate new or updated physical security measures.

Prevent

The presence of visible security features and operations may deter an adversary from attacking or disrupting an asset or corresponding components. Although it is difficult to determine the level of effectiveness of deterrence measures, visible security features and operations may help owners and operators prevent common minor incidents such as vandalism and theft. Deterrence measures (e.g., visible barriers, surveillance cameras, intrusion detection sensors, protective lighting, the presence of security officers) may help to deter an adversary and prevent an incident before it occurs. In addition to preventing unauthorized facility access, these security measures are designed to safeguard personnel.

Resources for Additional Information

- "Dams Sector Protective Measures Handbook" (FOUO) (Section 3: Risk Reduction Strategies and Appendix B: Crime Prevention Basics)
- "Emergency Preparedness Guidelines for Levees" (Section VI: Importance of Training and Exercises)

Physical security preparedness may also include identifying and ensuring the availability of materials, equipment, and personnel needed for an emergency response. Certain types of disruptions might result in temporary or permanent loss or incapacitation of key personnel, making the designation of decision-making authority in advance of various circumstances a critical component to preparedness. It may be necessary to identify whether any critical skills reside with just one individual such that loss of that person would seriously interfere with safe dam operations. In addition, personnel may need to operate, maintain, and patrol dispersed assets, such as those with multiple dams, remote control centers, navigation locks, or levee systems. As such, training and exercises can be periodically conducted to demonstrate actions to be taken during disruptions, as well as practical considerations and limitations that may otherwise be overlooked in a written security plan, but may be addressed in an EAP (Chapter 4: Personnel Security Practices provides more information on EAPs). Examples of security measures are described in greater detail under other general physical security functions listed below.

Detect and Assess

Implementation of security measures such as intrusion detection systems, monitored video surveillance systems, protective lighting, and electronic access controls may help to detect and assess a security incident. Security officers may also help to detect an event during patrols, but are often better suited to assessing events than performing incident detection. Nuisance and false alarm rates are often very high with detection systems; therefore, detection without proper assessment is typically not considered detection of an event.

Resources for Additional Information

- "Dams Sector Protective Measures Handbook" (FOUO) (Section 3: Risk Reduction Strategies)

Common examples of measures used for detection and assessment of physical security incidents are listed below. As many of these detection measures are technological in nature, owners and operators leveraging these types of measures may also consider hardening or otherwise securing (with physical reinforcement, barriers, or other non-technological protection) the energy supply required for operation.

- **Intrusion Detection System:** Intrusion detection systems include the use of sensors, alarm systems, personnel, andother methods to alert site personnel of unauthorized access to the site, area, or system. Detection equipment and the systems that coordinate that equipment can be leveraged to identify intrusions in a timely manner and accurately characterize them. Automated intrusion detection technologies are particularly beneficial in their ability to detect and catalog events more reliably than personnel alone over extended periods of time. However, personnel often excel at assessing situations and are an important component of every intrusion detection system.
- **Surveillance Systems:** Surveillance systems commonly incorporate both natural surveillance and electronic surveillance system characteristics into one effective program. Surveillance cameras are crucial to any security program, as they can provide the ability to witness and record incidents, which can help to identify suspects, protect against liability claims, and be used as an effective investigation tool. Furthermore, video analytics (i.e., the analysis of surveillance camera recordings) may be used to combine surveillance and intrusion detection systems data to enhance situational awareness and potentially detect otherwise unknown incidents or trends that may compromise physical security. The proper use of surveillance cameras is usually dependent on the minimum level and evenness of lighting; field of view; the angle at which the camera is installed; the camera type (e.g., thermal imaging, infrared, or lowlight); and the camera's optical properties, such as lens fixed focal length.
- **Protective Lighting:** Protective lighting is a critical physical security feature, as many malicious acts are committed during evening hours. The mere ability to detect and assess nighttime incidents may offer an additional deterrent by proactively preventing such attacks. In addition, proper protective lighting may improve the effectiveness of the surveillance system, depending upon the type of surveillance technology in use at the site.
- **Security Officers:** The available security forces (including onsite personnel and local law enforcement); their coverage of assets; and their ability to respond, interrupt, and neutralize adversaries are highly valued components of physical security. Owners and operators may choose whether the officers are to be onsite, armed or unarmed, contract officers or hired personnel, or some combination thereof. The choice of onsite security officers may require a significant investment to provide the necessary services, which could demand a large portion of a facility's security budget.

Delay and Deny

The delay function uses security measures that reduce an adversary's rate of advance until a response force can arrive and neutralize the incident. Typically, delay measures include locks, barriers, or other hardening features that impede an adversary's progress. Denying the adversary is accomplished by placing security features around an area or asset. The deny function is commonly based on the adversary's skill and tools, and it can be very expensive to implement impassible barriers around every critical asset. The effectiveness of delay and deny measures begins only once an adversary has been detected; delay prior to detection and assessment is typically not considered as part of the effectiveness of the delay function. Effective measures for delaying and denying an adversary include:

Resources for Additional Information

- "Dams Sector Protective Measures Handbook" (FOUO) (Section 3: Risk Reduction Strategies)
- ASCE "Guidelines for the Physical Security of Water Utilities and of Wastewater/Stormwater Utilities" (Appendix A: Physical Security Elements)

- **Entry Control Components:** Components that provide the ability to limit access to the site, sensitive assets (e.g., gates, transformers, or the dam), or sensitive buildings or rooms using a method to authenticate and approve all entry and access. Access is commonly provided on a need-to-access basis without alternate routes to the area. Vehicle barriers, fencing, door locks, electronic access control systems, and gates are all examples of entry controls. Key control programs support entry control for mechanical locks used to protect an area or facility, documenting the issuance of keys and assisting in the prevention of copying or loss of keys.
- **Electronic Access Control Systems:** Systems used to limit physical access to the facility, discrete parts of the facility, and/or its perimeter to authenticate and authorize personnel, contractors, vendors, temporary personnel, and visitors. Written policies are often implemented to ensure each individual has the proper level of access authorization using a need-to-access basis. Detailed protocols may be developed to define proper badging, authorizations, and recovery of issued badges. In addition, access control records may be considered security-sensitive data and are commonly secured and destroyed according to organization policy.
- **Barriers:** Doors, locks, windows, walls, roofs, floors, fencing, vehicle barriers, safes, vaults, and other related technologies designed to prevent or delay an adversary's path. Owners and operators use barriers to bolster vehicular entry points, perimeter protection, and pedestrian entry points to facilities or structures. Vehicle-rated barriers are commonly deployed to particularly sensitive points of entry, or when threat conditions increase. Barriers may also be used to support electronic access controls and provide proper standoff distances from critical areas or facilities. The use of gates, turnstiles, and other pedestrian barriers may help to limit access to critical assets and components. In addition, ventilation shafts and ducts, utility tunnels, and other similar enclosed pathways may be considered for additional barriers.
- **Blast Mitigation:** Hardening features that provide protection from explosions for facilities and/or specific areas. Specialized construction materials and films may be required, depending on the threat to the specific asset or area. Typically, barriers are implemented first, whenever possible, to provide standoff distance from critical assets and operations. If the use of barriers is not possible, owners and operators may consider blast mitigation measures, as appropriate.

Respond

Effective incident response and associated communications are critical for physical security. During an incident, swift and accurate communications to and among a response force are crucial. In addition, the time it takes for an effective response force to respond, interrupt, and neutralize an adversary is the basis for determining many requirements for physical protective measures. Therefore, understanding the response time for those responsible for protecting the site or project, such as local or state law enforcement officials, is an important step in implementing response security measures. The time it takes to detect, assess, communicate, and respond to the incident can dictate the type of security measures to be used to best protect critical assets.

Key measures for effective incident response include:

- **Communications:** The integration of the different security measures, technologies, and personnel is a vital part of managing and developing an effective protection program. Such integration includes day-to-day and redundant emergency communication systems and equipment for critical communication pathways. Communication methods often include wired and wireless networking to transmit security feeds from detection and surveillance systems. As a result, the convergence of physical and cybersecurity is increasingly common; a collaborative effort may be developed, enhanced, and promoted between information technology (IT) and security personnel. See *Chapter 3: Cybersecurity Practices* for more detail.
- **Response Forces:** Security personnel are the major component of effective incident response. A response force may include just one security or local law enforcement officer, or may be expanded to include dedicated teams of personnel trained and activated for specific events, such as Special Weapons and Tactics (SWAT) teams or law enforcement bomb squads. Response force requirements relative to specific facility or asset vulnerabilities may be identified in vulnerability assessments as described in the *Conduct Assessments* section of this chapter.

Resources for Additional Information

- "Dams Sector Protective Measures Handbook" (FOUO) (Section 3: Risk Reduction Strategies and Section 5: Protective Measures)
- Dams Sector "Emergency Preparedness Guidelines for Levees" (Section VIII: Managing Incidents: Structure and Responsibilities)
- FERC "Security Program for Hydropower Projects" (Section 7.4.1: Emergency Notification and Communications during a Security Incident)
- NERC "Security Guideline for the Electricity Sub-sector: Physical Security Response"

- **Safeguarding Personnel:** During an incident, controlling access and egress—such as through a physical security boundary—is designed to restrict entrance and exit movement to authorized personnel and resources. This provides protection not only for the facility, but also for personnel within the facility.

Restore

Certain facilities or projects, especially some large Federal dams, provide a wide range of economic, environmental, and social benefits to broad communities. Disruption of such projects for extended periods could have devastating economic impacts regionally or even nationally. Though smaller private dams might not provide the same level of regional benefits, there is still the potential for extensive impacts on local communities, as well as the financial impacts on the owners.

Resources for Additional Information

- "Dams Sector Crisis Management Handbook" (Section 5: Protective Measures, Section 6: Risk Management and Assessment, Appendix B: Recovery Plan Content Guidelines, and Appendix C: Continuity Plan Guidelines)

Efficient and effective restoration and recovery after an incident or disruption may mitigate the adverse effects of high-consequence events. Since it is difficult and expensive to prevent some of the greatest threats to critical assets, the ability to recover from a high-consequence event is paramount. Physical security measures in place for the restore function may often reduce the effects of an incident and, in some cases, may be the only way to effectively protect the project or its critical assets from certain threats. Examples include:

- **Resources:** Heavy equipment, stockpiles of replacement parts, and contractual support for recovery operations are highly valuable components that may be used to restore critical assets and functions.
- **Mutual aid:** Mutual aid agreements with other Dams Sector facilities or companies or with other critical infrastructure owners and operators (especially the Electricity Subsector and the Water and Wastewater Sector) are commonly leveraged in planning for recovery and restoration.

Comprehensive Physical Protection System and Procedures

Many sector owners and operators employ a comprehensive physical protection system to mitigate risks to their assets. A comprehensive system merges people, procedures, and equipment into a single methodology. Owners and operators may approach system integration by developing and maintaining a physical security plan, which describes all physical security measures and procedures to best ensure security within the full range of threat conditions. Similar assets may

need very different physical security measures and procedures—no two physical security plans are exactly the same. In addition, the physical security plan may be incorporated into a comprehensive site plan, as some owners and operators may choose to combine multiple strategic documents into one, including physical security, response, and recovery plans, as well as EAPs.

These plans often include provisions for personnel safety and security, especially relating to egress or evacuation from the site of an incident. A sample security plan outline is included in *Appendix F* and more extensive security plan templates are included in the "Dams Sector Protective Measures Handbook" (FOUO) and posted on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Dams Portal.

Resources for Additional Information

- "Dams Sector Security Guidelines" (Chapter 4: Personnel Security Practices)
- "Dams Sector Protective Measures Handbook" (FOUO) (Section 3: Risk Reduction Strategies, Section 4: Threats, Section 5: Protective Measures, Appendix A: Protective Measures in Relation to National Terrorism Advisory System Threat Level, and Appendix H: Security Plan Template)
- FERC "Security Program for Hydropower Projects" (Section 7.4: Internal Emergency Response and Rapid Recovery)

Emergency Action Plans

Emergency action plans (EAPs) are common strategic plans used by Dams Sector owners and operators. These plans broadly cover the safety of a facility or project and are often required by regulation. Though EAPs are intended for safety incidents, their content makes them valuable for planning or response related to security incidents. Because of common regulatory requirements for EAPs, many sector owners and operators already have plans, procedures, and measures in place at their facilities and projects. These can be incorporated into a comprehensive physical protection system. To maintain strategic plans in a single document, owners and operators may choose to include separate annexes for physical and site security within the facility or project EAP.

Regardless of how these strategic plans are organized, comprehensive physical protection systems are intended to be flexible and have the ability to change as the threat levels increase or decrease. A baseline level of security can be defined, maintained, and monitored. A sample of baseline measures that could be implemented for all facilities and enhanced measures for critical assets can be found in *Appendix D*. Example measures may be tailored for each individual facility. As threat conditions change, the system can be modified to effectively mitigate the associated risk (including periodic updates to threat identification portions of strategic plans). Owners and operators can develop active plans that, in advance, direct security resources and procedures for increasing levels of security protection as the threat landscape intensifies. This supports the ability to rapidly change the security posture for local and regional threats that may arise quickly based on specific issues in the area, such as a protest or localized increase in copper theft. Many sector owners and operators plan and prepare for at least four levels of security measures at their facilities.

- **Level 1:** The minimum (baseline) level of security at the facility or project to protect assets against anticipated incidents and ongoing threats.
- **Level 2:** Enhanced security measures at the facility or project in response to information received of a potential threat that exists to national critical infrastructure, but that is not specific to the Dams Sector.
- **Level 3:** Enhanced response, recovery, or security measures at the facility or project where information has been received concerning a potential threat to State- or local-level critical infrastructure, or when a national threat to the Dams Sector is communicated.
- **Level 4:** The highest level of security, response, and recovery measures at the facility or project to address a credible, specific threat communicated to the sector owner or operator that is specific to a State, local region, sector asset, or entity.

One approach to determining when to increase security measures is to follow the DHS NTAS alerts, which indicate whether the threat is elevated or imminent. If NTAS alerts indicate credible threats of terrorism related to the Dams Sector, owners and operators may choose to elevate their security measures. The NTAS Website (http://www.dhs.gov/national-terrorism-advisory-system) is the authoritative source for information about the current NTAS level. An NTAS Alert will be issued only when credible information is available and will be based on the nature of the threat. In some cases, alerts will be sent directly to law enforcement or affected areas of the private sector. In other cases, alerts will be issued more broadly to the American people through both official and media channels.

Defense-in-Depth

Defense-in-depth is another fundamental physical security concept commonly included in comprehensive physical protection systems. Defense-in-depth, also known as layered protection or protection in depth, is based on placing multiple layers of security features without gaps or weaknesses. Three general layers of defense accomplish a basic level of defense-in-depth (as demonstrated in Figure 5):

- **Outer Defensive Layer:** Often referred to as the outer perimeter, this layer consists of perimeter fencing, barriers, protective lighting, intrusion detection systems, surveillance systems, and other security measures used to deter, detect, assess, delay, and assist in an effective response to attacks.
- **Middle Defensive Layer:** This security layer comprises building exteriors, doors and locks, windows and utility openings, ventilation ducts, protective lighting, intrusion detection and surveillance systems, and other similar security measures.
- **Inner Defensive Layer:** Doors, windows, locks, intrusion detection systems, protective lighting, and other security measures are designed to protect against an adversary who has penetrated the outer and middle layers of protective measures. Inner layer protective measures may also protect against internal threats.

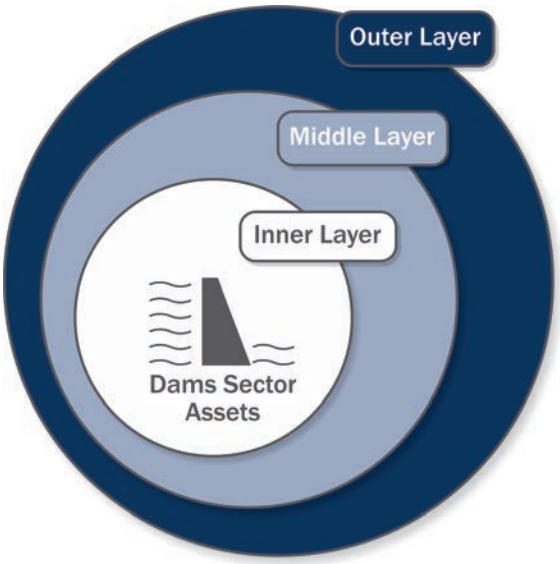


Figure 5. Example defense-in-depth layers surrounding Dams Sector assets

Defense-in-depth also implies that each layer of security has the same level of protection all the way around the asset; however, in the case of spatially-extended assets such as dams, the defensive layers provide protection along feasible attack paths, which may necessitate the delineation of additional defense layers. This builds redundancy into the integrated physical protection system; in the event a technology or process fails at one layer, there are more security features in place to protect the asset. When defense layers are changed or added, consideration is typically given to incorporating appropriate safety features to allow for exiting or evacuating nearby areas during an emergency.

Resources for Additional Information

- ASIS International: "Facilities Physical Security Measures Guideline" (Section 3.1.2: Strategies)
- NERC "Security Guideline for the Electricity Sector: Physical Security" (Protection In Depth)

3. Cybersecurity Practices

In addition to physical risks, the Dams Sector is exposed to cyber risks, with cyberattacks increasing in severity, frequency, and sophistication each year. Achieving security and resilience requires a collection of cyber and physical security practices adaptive to incidents occurring in the physical and cyber environments.

In embarking on a robust approach to cybersecurity, owners and operators identify critical cyber assets and systems, in addition to cyber risks and vulnerabilities. After identifying these cyber assets, systems, risks, and vulnerabilities, owners and operators can then implement cybersecurity practices designed to improve their cybersecurity posture, prevent or mitigate a cyberattack, and ensure the continuity of facility operations and services. Owners and operators may choose to concentrate on a particular cybersecurity function (e.g., detection or response), according to deficiencies uncovered through assessments, or they may develop and administer a comprehensive cybersecurity plan inclusive of the identify, protect, detect, respond, and recover functions.

Cybersecurity in the Dams Sector is primarily focused on the control systems that monitor, automate, and control critical physical processes such as electrical generation and transmission, water level and transport, and physical access. These control systems also collect information about operations and component status to manage, command, or regulate key components over digital networks (including the Internet and wireless networks). However, the security of control systems is not the only activity in the owner's or operator's cybersecurity portfolio. Compromising an IT system and its connecting networks and information could also bring an organization to a standstill, causing economic damage and jeopardizing the security of the facility and its personnel. As such, an effective cybersecurity framework accounts for threats to both control and IT systems and their connecting networks and information.

The first step in cybersecurity risk management is to identify cyber assets and systems. This entails identifying and documenting all network infrastructure, devices, applications, data storage, data flows, and all connections to the control systems. Once identified, assets and systems are then assessed. Based on the results of cybersecurity assessments, particular components can be selected for more thorough analysis of cybersecurity vulnerabilities and threats. This is then followed by the implementation of cybersecurity measures through a comprehensive cybersecurity framework. It is important that, throughout all cybersecurity risk management activities, owners and operators remain cognizant of the cyber-physical dependencies and relationships that exist within and connect to their facilities and assets. A successfully implemented cybersecurity framework encompasses information sharing taking place among management and operations personnel operating within the physical and cyber space. This level of information sharing can be achieved through such activities as regular conference calls, cross-discipline working groups, or co-location of personnel.

Cybersecurity Framework

Resources for Additional Information

- "Dams Sector: NIST Cybersecurity Framework Implementation Guide"
- NIST "Cybersecurity Framework"

Adversaries can exploit the increased complexity and connectivity of Dams Sector critical infrastructure systems to cause their improper operation, which may place the security, economy, public safety, and public health at risk. There are many attack types and vectors that can be used to cause economic and operational damage. Adversaries can infiltrate data processing, transfer, and storage systems, and then alter, corrupt, or steal information. Information systems can be attacked with the intent of overloading the equipment (e.g., denial-of-service attacks), and some information systems can be used to initiate attacks on other systems (e.g., botnet attacks). In addition, industrial control systems, such as supervisory control and data acquisition (SCADA) systems, can be compromised and manipulated to operate equipment in such a way as to cause damage and inflict onsite and offsite

casualties. Adversaries can also hack a cyber system to gain information about facilities or personnel, use the system as a surveillance tool, or coordinate a cyberattack with a physical attack. To better address these threats, owners and operators can conduct cybersecurity assessments—many of which are available free of charge—and implement a cybersecurity framework, such as the National Institute of Standards and Technology (NIST) "Cybersecurity Framework."

As owners and operators increasingly rely on cyber assets and systems, and as adversaries become more sophisticated and bolder in attacks, the criticality of implementing cybersecurity practices increases. On February 12, 2013, Executive Order 13636 (EO 13636): Improving Critical Infrastructure Cybersecurity was issued, which called for the development of a voluntary cybersecurity framework that provides a prioritized, flexible, repeatable, and cost-effective approach to managing cybersecurity risk. The NIST "Cybersecurity Framework" is an approach that will help owners and operators to:

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state; and
- Communicate among internal and external stakeholders about cybersecurity risk.

The NIST "Cybersecurity Framework" broadly applies across all organizations, regardless of size or cybersecurity sophistication. The Dams Sector developed the "Dams Sector: NIST Cybersecurity Framework Implementation Guide" to help organizations understand and use the framework as it applies to their particular industry.

Conduct Cybersecurity Assessments

The key to robust cybersecurity is to conduct assessments to identify cybersecurity risks and evaluate the organization's cybersecurity practices and cyber-operational resilience. For dams, it is important to determine whether an automated control system could be remotely manipulated to cause improper operation and whether improper operation could cause significant damage or destruction. Cybersecurity assessments may be conducted as self-assessments or as onsite assessments facilitated by cybersecurity professionals. By conducting cybersecurity assessments, owners and operators will have a better understanding of their cybersecurity posture, where system vulnerabilities exist, and what actions are required to address them. This empowers owners and operators to prevent or mitigate the consequences of a cyberattack, such as equipment damage, loss of hydropower generation, serious damage to major dam components, or manipulation of the security environment. Effective and accepted cybersecurity assessment tools include:

Resources for Additional Information

- "Dams Sector Roadmap to Secure Control Systems" (Appendix C: Industrial Control System Details/Assessing Risks of Critical Cyber Elements)
- Dams Sector C2M2 (to be released in 2015)
- Electricity Subsector C2M2
- ICS-CERT Cyber Security Evaluation Tool (CD, onsite training, guidance)
- US-CERT Cyber Resilience Review (onsite assessment, self-assessment resources)

- **Dams Sector Cybersecurity Capability Maturity Model (C2M2):** C2M2 is a no-cost, voluntary tool utilizing industry-accepted cybersecurity practices to assess an organization's cybersecurity capabilities and prioritize actions and investments to improve their cybersecurity posture. C2M2 supports the adoption of the NIST "Cybersecurity Framework" and also assesses domains similar to that of the Cyber Resilience Review (see below).
- **Cyber Security Evaluation Tool (CSET):** Offered by DHS, CSET is a no-cost, voluntary desktop software tool designed to guide users through a step-by-step process to assess their control systems and IT network security practices against recognized industry standards. The user selects one or more of the government and industry recognized cybersecurity standards (e.g., "NERC Reliability Standards CIP-002-009" Version 5), which will generate assessment questions specific to the selected requirements. The tool then compares completed answers with the recommended requirements from the standards selected. After assessment completion, a prioritized list of recommendations for improving the organization's cybersecurity posture and associated actions to be taken will be made available.

- **Cyber Resilience Review (CRR):** Offered by DHS, the CRR is a no-cost, voluntary, non-technical assessment designed to evaluate an organization's cyber-operational resilience and cybersecurity practices across 10 domains. Although the CRR predates the NIST "Cybersecurity Framework," most of the assessed CRR practices align closely with the framework. The CRR can be used to evaluate the resilience capabilities of enterprises with highly defined and mature operational resilience capabilities, as well as organizations with less defined and mature capabilities. Owners and operators can also choose to download the free self-assessment or schedule an onsite assessment facilitated by trained DHS cybersecurity professionals; both options generate a final report inclusive of options for consideration and the organization's maturity level relative to the assessed domains.

Implement Cybersecurity Measures

Complete cybersecurity is achievable only through the implementation of robust and enduring cybersecurity measures organization-wide. To facilitate the achievement of secure cyber assets and systems, owners and operators can consult the FERC "Baseline Cyber Security Measures," the NERC "CIP Cyber Security Standards," and the NIST "Cybersecurity Framework." While the FERC and NERC measures represent singular industry-accepted standards, the NIST "Cybersecurity Framework" represents a framework built from many existing standards, guidelines, and best practices. It outlines five cybersecurity core functions designed to achieve specific cybersecurity outcomes and references examples of how to achieve those outcomes. This section is organized by the five core functions designed to facilitate cybersecurity risk management: identify, protect, detect, respond, and recover.

Resources for Additional Information

- "Dams Sector: NIST Cybersecurity Framework Implementation Guide"
- NIST "Cybersecurity Framework" (Appendix A: Framework Core)
- "Dams Sector Crisis Management Handbook" (Appendix C2: Computer Incident Response Guidelines)
- NERC "CIP Standards – Cyber Security (CIP-002-3 – 009-3)"
- FERC "Security Program for Hydropower Projects" (Section 9.3: Security Measures for Cyber Assets)

Core Functions of the NIST "Cybersecurity Framework"
Identify: Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The protect function limits potential cybersecurity events.
Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, enabling the timely discovery of cybersecurity incidents.
Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The respond function supports the ability to contain the impact of a potential cybersecurity event.
Recover: Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services impaired by the cybersecurity event.

Identify

Similar to other critical infrastructure, dams employ a variety of industrial control systems—such as SCADA and distributed control systems—to monitor, automate, and control critical physical processes. Dams also utilize a variety of networks and IT systems with networked information in their daily operations.

These control and IT system assets represent the linchpin for operational facilities, and identifying them is critical. The identification phase involves documenting and evaluating the criticality of the entire network infrastructure, devices, applications, data storage, data flows, and all connections to the cyber assets and systems. For each cyber asset and system, the

NIST Cybersecurity Function: Identify
Asset Management: Identification and management of cyber assets and systems.
Business Environment: The facility's organization, mission, and objectives used to inform cybersecurity roles, responsibilities, and risk management.
Governance: The facility's policies, procedures, and processes used to inform cybersecurity risk.
Risk Assessment: Understanding of cybersecurity risk to operations, assets, and individuals.
Risk Management Strategy: Establishment of priorities, constraints, risk tolerances, and assumptions and their use for risk decisions.

criticality to the facility's operations is evaluated, and owners and operators may then classify the asset or system as critical or non-critical. When it is more convenient to classify the criticality of the cyber assets as a group, then the criticality of the cyber system as a whole is evaluated instead of the criticality of each individual asset. Cybersecurity measures under the identify function may include identifying and documenting cyber asset vulnerabilities and internal and external threats.

Protect

Within the Dams Sector, control systems are used either onsite or remotely to control and/or monitor operations. They are subject to issues that complicate their protection: increased connectivity, interdependencies, complexity, legacy systems, wireless connection and communication, offshore reliance, and information availability. In addition to cybersecurity measures protecting control systems, measures need to be in place to prevent or mitigate the various types of cyberattacks, which may be more pervasive than just an attack on control systems. In this phase, protective cybersecurity measures are implemented to protect from several types of cyberattacks: automated cyberattacks (e.g., software attacks from worms, viruses, or Trojan horses), external cyberattacks (e.g., outside individual gaining unauthorized access), or internal cyberattacks (e.g., personnel or contractors/vendors gaining unauthorized access). The criticality determined in the identification phase will decide the level of security measures, such as baseline or enhanced, that should be implemented for the cyber assets or systems. Protective cybersecurity measures may include identifying and credentialing authorized devices and users and remotely managing cyber assets and systems.

NIST Cybersecurity Function: Protect
Access Control: Access to assets and facilities is limited to authorized users, processes, or devices.
Awareness and Training: Employees and contractors receive cybersecurity awareness and information-security responsibility training.
Data Security: Information and data are managed according to the facility's risk strategy.
Information Protection Processes and Procedures: Security policies are used to manage the protection of information systems and assets.
Maintenance: Maintenance and repair of control systems is performed.
Protective Technology: Technical security solutions are managed to ensure system security and resilience.

Detect

Protective measures may sometimes be insufficient to prevent or mitigate nefarious cyber activity. As such, capabilities to detect cyber-intrusion activity, misuse, or negligence are critical to containing the activity and ensuring an appropriate response level. In this phase, detection technology and procedures are implemented to discover abnormal conditions with IT systems and networks using a strategy of continuous monitoring and detection. This function of cybersecurity is intended to enable the ability for rapid response to limit the potential damage of a cyber incident. Embracing a defense-in-depth cybersecurity approach (also referred to as layered protection) includes not only measures to protect against any single point-of-failure types of breaches, but also intrusion detection strategies and technology. Detection cybersecurity measures may include establishing and managing a baseline of network operations and expected data flows and conducting regular vulnerability scans.

NIST Cybersecurity Function: Detect
Anomalies and Events: Abnormal activity is detected in a timely manner, and potential impact is understood.
Security Continuous Monitoring: Information systems and assets are monitored at distinct intervals.
Detection Processes: Processes and procedures are maintained and tested to ensure timely awareness.

Respond

Despite the implementation of cybersecurity measures for protection and detection, a cyber incident compromising asset or facility security may occur. In the event of an incident, the owner or operator seeks to take appropriate action in response to the detected cyber incident. Response cybersecurity activities may include executing a cyber incident response plan and mitigating newly identified vulnerabilities or documenting them as accepted risks. Along with short-term activities specific

to the incident recovery phase, a typical response plan might include other processes:

- Determine the nature of the incident
- Determine whether the incident is malicious or non-malicious in origin
- Analyze available data sources
- Respond:
  - Isolate the compromised host
  - Block malicious traffic with existing security devices
  - Patch/harden infrastructure to address the specific vulnerability
  - Report to law enforcement if criminal activity is suspected
- Recover:
  - Recover the compromised hosts
  - Survey infrastructure for other vulnerable hosts
  - Patch/harden as appropriate
  - Quantify loss if seeking legal remedies
  - Monitor host and network for signs of subsequent compromise
  - Conduct post-mortem analysis
  - Revise procedures and training based on post-mortem analysis

NIST Cybersecurity Function: Respond
Response Planning: Response processes and procedures are executed and maintained.
Communications: Response activities are coordinated with internal and external stakeholders, including law enforcement.
Analysis: Analysis is conducted to ensure adequate response and recovery.
Mitigation: Expansion of the event is prevented, its effects are mitigated, and the incident is eradicated.
Improvement: Facility response activities are improved by incorporating lessons learned from the detection and response phases.

To ensure an effective cyber response, checklists can be developed for teams to respond to various types of cyber incidents. The lists could include other useful information, such as command post locations and instructions for obtaining information updates during the response. In addition, the cyber incident response plan should be reviewed and updated, and the response process tested regularly. In simulating a cyber incident, a tabletop exercise might be considered.

Recover

With the increasing importance of cyber assets and systems to facility operations, rapid recovery is critical to mitigate disastrous effects and maintain business continuity. In this phase, the owner or operator seeks to restore critical assets and operations to ensure the continued operation of the asset, which might include the execution of recovery plans to bring critical services online quickly. Recovery cybersecurity activities may include executing a recovery plan, managing public relations, and communicating recovery activities to internal stakeholders and executive and management teams. Critical to the recovery phase are post-incident evaluation activities, which may include:

- Collect necessary information/evidence
- Determine the cause of the incident
- Determine the effects of the incident
- Make recommendations for improvements to the systems
- Make recommendations for improvements to the incident response

NIST Cybersecurity Function: Recover
Recovery Planning: Recovery processes and procedures are executed and maintained.
Improvement: Facility recovery activities are improved by incorporating lessons learned.
Communications: Restoration activities are coordinated with internal and external parties, including coordinating centers, Internet service providers, owners of systems actively attacking, affected systems, other computer security incident response teams (CSIRTs), and vendors.

4. Personnel Security Practices

The effectiveness of all Dams Sector security operations—including those for physical, cyber, personnel, or information security—is dependent on the people who perform and manage such efforts throughout the sector each day. Owners, operators, personnel, and contractors all perform mission-critical tasks to implement dam security measures and maintain mission integrity. Such high levels of responsibility necessitate appropriately high levels of scrutiny, training, and education because the errant or illicit actions of one person can cause catastrophic damage to assets, facilities, and the surrounding communities and environment.

Assessing threats includes screening potential and new hires or contractors for specific security risk criteria, periodically rescreening personnel, and determining the likelihood of, and vulnerability to, insider threats. The results of these activities inform owner and operator decisions on implementing personnel security measures such as background investigations, training to increase security awareness and education, and exercises and drills to hone skills and knowledge related to specific types of security incidents. Though not explicitly associated with personnel security risks and incidents, the development and management of response and recovery plans are included in this chapter as important drivers of personnel functions applicable to all-hazards incidents.

Conduct Personnel Risk Assessments

Risk assessment for personnel security within the Dams Sector is primarily focused on the risks posed by existing or potential personnel to the secure operation and maintenance of facilities and assets. Major portions of common risk assessment practices regarding sector personnel include screening potential hires and existing personnel (employees and contractors) for risk factors in individuals' characteristics and history, periodic rescreening of personnel for the same risk factors using a screening program, and examining the potential for deliberate malicious activity by personnel. The results of such assessments can be used to inform decisions about personnel and hiring changes, as well as to identify areas in which new or additional personnel security measures may be warranted. (See the Implement Personnel Security Measures section of this chapter for more information.)

Screening and Rescreening

Many owners and operators develop effective hiring policies that include an initial background screening to evaluate a potential candidate's character, employment qualifications, and fitness for the position being sought. A background screening can also be used to investigate any potential hiring risks for safety and security reasons.

Resources for Additional Information

- "Dams Sector Personnel Screening Guide for Owners and Operators"

Typically, such screening includes items such as past employment verifications, criminal history, and credit checks. The position being sought, the level of security required, and the access to critical assets and operations will determine the level of appropriate screening. Sector owners and operators may choose to develop a standard program for all personnel screening and rescreening to provide consistency, track information over time, and eliminate any potential for discrimination or prejudice. Basic elements of an effective personnel screening program may include:

- Consistent use of a standard application form or specialized forms as site specifics warrant;
- A definitive and rigidly enforced policy regarding which applicants must complete certain forms and background checks;

- A clearly stated and consistently enforced policy that failure to agree to a required background check will result in rejection of the application;
- A clearly outlined process for receiving applications, reviewing them for completeness, making acceptance or rejection decisions, documenting the decisions, and maintaining records of them;
- Precise definitions of any terms used to designate differing levels of access to facility equipment, buildings, records, computer systems, and control systems;
- Background check procedures and questions that comply with applicable Federal and/or State laws, any union agreements, and organization policy;
- Trained individuals to adjudicate investigative results and make decisions or recommendations regarding hiring of individual applicants;
- Standardized acceptance and rejection form letters;
- Clearly stated criteria for which applications will be rejected; and
- A precisely stated appeals process for rejected applicants.

Properly screening personnel may assist in mitigating some risk to the organization; however, it does not eliminate all risks and threats posed by vetted personnel and contractors.

Insider Threat

Insider threat can be defined as the probability of an attack facilitated or carried out by an individual with privileged access or information pertaining to a facility or asset of importance. Insiders may hold any position in an organization (e.g., physical protection system designer, security guard, clerk, IT specialist, operational and maintenance worker, or senior manager). Other individuals not directly employed by the owner or operator, but also have access to the facility or systems (e.g., vendors, contractors, subcontractors, and visitors), may also be an insider threat.

Resources for Additional Information

- "Dams Sector Protective Measures Handbook" (FOUO) (Section 4: Threats)
- "Dams Sector Security Awareness Handbook" (FOUO) (Section 4: Potential Indicators of Threat Activity)
- ASCE "Guidelines for the Physical Security of Water Utilities and of Wastewater/Stormwater Utilities" (Section 1.1.2.4: Insider)

Insiders may have access to and knowledge of some or all areas of a facility, its systems, and equipment; authority over operations or personnel; and technical skills and experience. Insiders often have knowledge of a facility's security features, which could be used to circumvent security measures in order to disrupt operations. An insider may be a hardworking, trusted employee for many years before deciding to attack his or her own organization. As a result, the insider threat may be the most difficult threat to identify and mitigate prior to an attack.

An effective program for assessing personnel related to insider threats may include:

- Procedures to properly evaluate personnel and contractor information, including consultation with the facility's or organization's legal counsel, human resources, and civil liberties and privacy officials to ensure compliance with all applicable laws and privacy requirements;
- Compliance assessments of personnel regarding insider threat policies and procedures to ensure the program is working as intended; and
- A process to facilitate the sharing of information from human resources, intelligence, law enforcement, and other pertinent sources to recognize the presence of an insider threat.

Appropriate measures to mitigate insider threats uncovered by personnel risk assessments are provided in the following *Implement Personnel Security Measures* section.

Implement Personnel Security Measures

Effective practices for personnel security in the Dams Sector, commensurate with personnel risk assessments, generally adhere to the fundamental risk management concepts of prevent and prepare, detect and assess, delay and deny, and respond and recover. Owners and operators conduct background investigations, training, and exercises, as well as incorporate lessons learned (from past incidents, training, and exercises), to better prepare personnel for security incidents and potentially prevent some incidents from occurring at all. Security awareness training, insider threat considerations, and standardized suspicious activity reporting are all effective means for detecting and assessing existing or potential personnel security incidents.

Physical security measures identified in *Chapter 2: Physical Security Practices* to delay and deny an adversary's progress through a facility or project are also relevant for supporting personnel security. Response and recovery planning, including EAPs and recovery plans— bolstered with a commonly understood and observed incident management and command structure— gives owners and operators clear pathways and procedures to maximize effective response and recovery and minimize incident consequences to facilities, assets, and communities.

Prevent and Prepare

Emergency incidents at dams (e.g., dam failures) are not common events. Therefore, training and exercises are necessary to maintain operational readiness, timeliness, and responsiveness. In addition, effective training and exercises may prevent personnel-caused security incidents from occurring. If such incidents do occur, clearly documenting and incorporating lessons learned from the incidents enhances the capability of sector owners, operators, and other personnel to prevent similar incidents from occurring again.

Resources for Additional Information

- Dams Sector Training Schedule (managed by the Dams Sector-Specific Agency)
- Homeland Security Exercise and Evaluation Program Website
- "Dams Sector Crisis Management Handbook" (Section 7: Exercises)

- **Procedural Considerations:** When applicable, owners and operators may choose to develop procedures to require segregation of duties or delegation of authority for the operation of critical assets so that one employee does not control the entire process for critical operations. This will ensure continuity of critical operations in emergency situations resulting in the temporary or permanent loss or incapacitation of key personnel, and will reduce the probability of personnel error in critical functions. For example, if communications are disrupted with the chief hydrologist (or the hydrologist is otherwise incapacitated) during a heavy rain incident, the onsite supervisor can be expected to open the gates.
- **Training:** The proper training of personnel and contractors/vendors is critical to the success of every organization. Training provides personnel with the knowledge, skills, and abilities to effectively perform key tasks to better accomplish the organizational mission. Owner/operator security training decisions can be based on information compiled from assessments, planning, and operations while using best industry practices as guidelines. Including baseline security awareness training is a means of instilling a common culture of security awareness among personnel. More detail on security awareness training is provided below in the *Detect and Assess* portion of this section. Well-informed and well-aware personnel may be able to recognize situations or conditions that have the potential to lead to a security incident and take corrective actions to prevent the incident from occurring. To assist owners and operators with training, the Dams Sector has developed online training modules based on three sector handbooks ("Security Awareness," "Protective Measures," and "Crisis Management") to provide stakeholders with information on security vulnerabilities, enhance their ability to assess the risks to their respective facilities, and improve their incident response capabilities.
- **Exercises:** The development and execution of exercises and drills in preparation for potential security incidents is a critical factor in determining the effectiveness of the overall security measures of a facility or project. Through exercises, organizations validate security plans, test operational capabilities, assess leadership effectiveness, and examine the various ways to prepare and respond to incidents. Essential exercise-related activities include preparing the exercise, managing exercise activities, and conducting immediate wrap-up activities such as lessons learned. To assist the owner or operator in preparing for and managing exercises and drills, DHS has implemented the Homeland Security Exercise and

Evaluation Program (HSEEP). HSEEP offers a common exercise policy and provides program guidance that constitutes a national standard for exercises. HSEEP includes consistent terminology that can be used by all exercise planners, regardless of the nature and composition of their sponsoring agency or organization. This program offers useful tools that exercise managers can use to plan, conduct, and evaluate exercises to improve overall preparedness.

- **Lessons Learned:** Documenting and leveraging past information regarding incidents and exercises is an important way to better prepare for future events or potentially prevent certain types of incidents from happening. Capturing lessons learned and creating an archive is an effective method for developing and improving a site's security posture. Understanding what went right and wrong may greatly reduce the chances of repeating past mistakes. Sector owners and operators often develop formal, documented lessons-learned processes that are updated as needed to capture this critical information. Formal meetings are also employed to discuss, capture, document, and share lessons learned after each incident or exercise. The meetings may include many topics, such as successes and why they were successful; failures and why they occurred; processes that should be kept, revised, or discarded; and what processes or actions could have been improved (e.g., efficiency, costs, protection, or response). The focus of these efforts is to capitalize on past successes or failures to improve the overall security of a facility or project.

Detect and Assess

In order to appropriately identify and evaluate personnel security risks and incidents, owners and operators commonly combine general security awareness training, insider threat policies and measures, and suspicious activity reporting.

Resources for Additional Information

- "Dams Sector Security Guidelines" (Chapter 5: Information Security Practices)
- "Dams Sector Security Awareness Handbook" (FOUO) (Section 3: Potential Indicators of Threat Activity and Section 4: Reporting Incidents)
- Dams Sector Training Schedule (managed by the Dams Sector-Specific Agency)
- Dams Sector Suspicious Activity Reporting Website

- **Security Awareness Training:** Security awareness training is based on the need to inform personnel (including contractors) of security risks and their specific responsibilities for complying with security policies and procedures. It is important that training requirements be set and documented for every employee and contractor, as the needs may vary based on each individual's role and responsibilities.

  Major subject areas for security awareness training commonly include cybersecurity, physical security, insider threat, terrorism and criminal activity, workplace violence, and active shooter. Key areas for consideration when developing a security awareness training program include:
  - Require annual (at a minimum) security awareness training and testing;
  - Maintain a central location for training resources and documentation;
  - Define total annual hours of training required per position type and responsibilities;
  - Develop incentive programs for training compliance and innovation; and
  - Implement visitor security awareness requirements, as appropriate.

- **Insider Threat Policies:** Dams Sector owners and operators understand the importance of detecting insider threats and assessing personnel actions and behaviors for the potential of insider threats. Standardized and documented insider threat identification and evaluation policies and procedures may reduce the probability of an insider attack as well as minimize the length of time between insider threat detection and mitigation. Effective approaches to detecting and assessing insider threats include technological monitoring and auditing of personnel access control (e.g., movement through controlled doors, locks, and barriers) and computer network use for activities or patterns of activity that may indicate an insider threat. Also, owners and operators may choose to implement an integrated, centralized reporting and response program to detect and mitigate insider threats. This may include the protocols and required documentation for investigating allegations of insider threats, all of which are approved by the organization's legal counsel, human resources, security management, and civil liberties and privacy officials.

- **Suspicious Activity Reporting:** Communication with personnel and vendors about security concerns and suspicious activities is crucial to the overall security of the facility or project. The acknowledgment of a suspicious activity may be the first indication that an illicit malicious event may occur. Therefore, owners and operators may choose to develop

and implement a method for employees and trusted vendors or contractors to report security-related incidents and suspicious activity. More detail on suspicious activity reports (SARs) is provided in *Chapter 5: Information Security Practices*.

Delay and Deny

Sector personnel may employ physical security measures to delay the advancement of an adversary or deny the adversary's access to sensitive areas or assets in a facility or project. It is important to consider that some established safety measures may conflict with physical security measures. The *Implement Security Measures* section of *Chapter 2: Physical Security Practices* provides delay and deny examples of entry control components, electronic access control systems, and barriers.

Respond and Recover

The close coordination of a facility's or project's personnel in the aftermath of a security incident is imperative for effective response and recovery. The actions taken by personnel after an incident has occurred can make the difference between minor consequences and major catastrophes. As a result, owners and operators readily employ extensive planning for incident response and recovery. The most common type of response plan across the sector is the EAP (as it is also a regulatory requirement for many facilities and projects). Recovery plans are also prominently featured and are often included within an EAP. These plans provide a consistent, commonly understood structure and process by which sector personnel can take corrective and mitigation actions. Personnel safety and security is paramount during an incident, and so response and recovery plans commonly include stipulations for maintaining personnel safety during egress or evacuation from an incident. Roles and responsibilities of specific personnel, including specialized response or recovery teams, are a major component of response and recovery plans, which typically include portions relating to Federal incident management guidance such as the National Incident Management System (NIMS) and its Incident Command System (ICS) component.

Resources for Additional Information

- "Dams Sector Protective Measures Handbook" (FOUO) (Section 3: Risk Reduction Strategies and Section 5: Protective Measures)
- "Dams Sector Crisis Management Handbook" (Section 5: Recovery Plans)
- "Emergency Preparedness Guidelines for Levees: A Guide for Owners and Operators" (Section VIII: Managing Incidents Structure and Responsibility)
- FERC "Security Program for Hydropower Projects" (Section 7.4: Internal Emergency Response and Rapid Recovery and Appendix F: Recovery (Response) Plan Format)
- FEMA "Federal Guidelines for Emergency Action Planning for Dams" (Section 1: Basic Considerations for Preparing an Emergency Action Plan)
- National Incident Management System and Incident Command System Website

- **National Incident Management System:** NIMS provides a proactive approach to systematically assist all levels of government, utility providers, and private sector organizations to work seamlessly in response to incidents. The NIMS approach is effective for any situation that involves coordination among multiple agencies or partners. The goal is to coordinate activities to reduce consequences (loss of life, property damage, and harm to the environment).

  ICS is a core element of NIMS and is composed of a standardized, on-scene, all-hazards incident management approach that allows for the integration of personnel, procedures, facilities, equipment, and communications operating within a common organizational structure. ICS also enables a coordinated response among jurisdictions and agencies, both in the public and private sectors. Further, it establishes common processes for planning and managing resources and proper budgetary allocations.

  Owners and operators often incorporate NIMS and ICS information into an EAP and/or a recovery plan. This allows all users to easily reference the needed information in a single location.

- **Emergency Action Planning:** "Federal Guidelines for Emergency Action Planning for Dams" (also referred to as FEMA 64) defines EAP as a formal document that identifies potential emergency conditions at a dam and specifies actions to be followed to minimize loss of life and property damage. The EAP typically contains the information necessary to guide owners and operators in preventing, responding to, and mitigating impending incidents and minimizing any ensuing life safety consequences and property damage. Common elements worth considering for an EAP include (but are not limited to):

- Actions the facility or project owner will take, in coordination with emergency management authorities, to mitigate a problem, risk, or emergency incident at the dam.
- Procedures owners will follow to provide early warning and notification to responsible downstream emergency management authorities.
- Delineation of the responsibilities of all those involved in managing an incident or emergency and how the responsibilities should be coordinated and communicated.

In addition, inundation maps may be included to help owners and emergency management authorities identify critical infrastructure and population-at-risk sites that may require protective measures, warning, and evacuation planning.

Annual EAP exercises and annual reviews and updates of the EAP—as well as the subcomponent plans it may contain (e.g., recovery, security, and/or evacuation plans)—are valuable means to maintain the EAP's relevance and effectiveness of associated response and recovery policies and procedures.

- **Recovery Planning:** The establishment of a recovery plan can help to minimize downtime and further reduce potential economic consequences from incidents for owners and operators. These plans detail the processes and information the owner needs to efficiently and effectively respond to many adverse events. Recovery plans enable owners and operators to more quickly mitigate, recover, and reinstate essential project services and functions, which will be beneficial not only to the owner, but also to the region and Nation.

  A recovery plan differs from an EAP in that it is more specifically focused on the response and recovery aspects of an event. Typically, the EAP covers a much more robust set of documentation spanning a very wide spectrum of emergency situations. Common elements shared by EAPs and recovery plans include processes and protocols for defined types of emergency scenarios, an incident command system with assignment of responsibilities, coordination with local authorities, and primary and backup communications equipment. Other common elements include drawings, maps, and photographs of facilities and assets to aid in response; sources and availability of vehicles, equipment, materials, supplies, and contractors; and estimated response times per incident type.

- **Response and Recovery Teams:** Depending on the type and severity of an incident at a facility or project, appropriate response and recovery measures are indicated by owners and operators and their response and recovery plans. For some incidents, specifically defined teams of personnel may be called upon to perform the response and recovery measures deemed necessary. Personnel may include local law enforcement or an onsite security force.

  For many Dams Sector facilities and projects, local law enforcement personnel are the only security force available for response (see the *Response Forces* portion of the Implement Security Measures section of Chapter 2). Routine coordination and collaboration with local law enforcement by owners and operators is therefore important to facilitate adequate understanding of the facility and mission, as well as security threats.

  Owners and operators may also consider appointing a recovery team to plan and oversee the long-term recovery process. The team would comprise members experienced with evaluation of structures, systems, equipment, and operations to develop alternatives to be considered and approved for returning to normal operations.

5. Information Security Practices

Information security is a critical component of any set of robust security practices. A facility without the proper information security measures in place could be subject to actors exploiting vulnerabilities with nefarious intent. For instance, stolen or incorrectly disseminated operational and proprietary information could be used to harm or disrupt facility functions or business operations at large. Information security measures are designed to prevent such consequences and protect information assets—both physical and electronic—from unauthorized access, use, disclosure, disruption, modification, inspection, or destruction. In addition to protecting information, the constant flow of information (e.g., threat environment, operating and environmental conditions, risk assessment results, and incident alerts and updates) is critical to the security of dam facilities, as well as the sector as a whole.

The first step to information security is to identify and document the landscape of physical records and information systems and associated electronic data. Information assets may include—but are not limited to—company reports, personally identifiable information (e.g., biographical data, names, addresses), network topology or similar diagrams, facility floorplans, or risk assessment results. Once identified, this information is used to conduct a risk assessment, which will enable the owner and operator to prioritize information security needs and to focus resources on the most critical gaps or vulnerabilities. The results of the assessment inform the implementation of information security measures, of which the "identify" and "protect" activities are the most important.

Conduct Information Security Risk Assessments

One of the major outputs for conducting a risk assessment of an organization's information security practices is an evaluation of the mitigation cost compared to the effects of consequences. An effective risk assessment will assist the owner and operator to prioritize information security needs and to focus resources on the most critical information security needs for both electronic and physical information. Considering that information security encompasses both the electronic and the physical sides, information security assessment activity may be incorporated under the cyber risk assessment approach, as described in Chapter 3: Cybersecurity Practices, or under the physical risk assessment approach, as described in Chapter 2: Physical Security Practices. However, the abundance of information located on and connected to information networks and the complexity inherent to the cyber environment calls for special attention to be paid to electronic information and its connection to physical assets. The following information outlines approaches to assessing electronic and physical information security.

Resources for Additional Information

- ICS-CERT Cyber Security Evaluation Tool (CD, onsite training, guidance)
- US-CERT Cyber Resilience Review (onsite assessment, self-assessment resources)
- Dams Sector Cybersecurity Capability Maturity Model (C2M2) (self-assessment, guidance, toolkit)

Assessing Electronic Information

- **Dams Sector Cybersecurity Capability Maturity Model (C2M2)** provides a benchmark that an organization can evaluate cybersecurity capabilities, some of which have a nexus to information security.
- **Cyber Security Evaluation Tool (CSET)** allows for the assessment of operational and information systems, which are likely to contain sensitive information. Various government and industry accepted standards, inclusive of information security standards, can be selected for evaluation.

- **Cyber Resilience Review (CRR)** enables the owner and operator to evaluate cyber-operational resilience and cybersecurity practices across 10 domains, most of which include the evaluation of information assets against information security goals and practices.

Assessing Physical Information

Facilities may hold physical information, such as personnel records and security plan documentations. Information assets are but one type of physical assets that require protection. In assessing the risk to physical information assets, the owner and operator may follow the guidance outlined in *Chapter 2: Physical Security Practices*.

Implement Information Security Measures

Information security measures are designed to protect information assets, regardless of whether they are in physical or electronic form, from unauthorized access, use, disclosure, disruption, modification, inspection, or destruction. Given the unique relationship of information security to cybersecurity, many of the security measures implemented under cybersecurity will also address information security. As such, the owner and operator may review the contents in *Chapter 3: Cybersecurity Practices* for additional information on implementing information security measures. This section engages with two critical components of the approach to information security: identifying information assets and protecting those assets.

Identify

The first step to implementing information security measures is to identify and document the landscape of physical records and information systems and associated data. Typically, information is stored in a protected manner based on the sensitivity and confidentiality of the information. Owners and operators may, if needed, develop standards for identifying information assets as sensitive in nature and thus requiring some level of protection from inappropriate or inadvertent disclosure. For examples of information assets, see Table 1—Examples of Potentially Sensitive Information and Table 2—Examples of Sensitive Information in the NERC "Security Guideline for the Electricity Sector: Protecting Sensitive Information."

Resources for Additional Information

- "Dams Sector Security Guidelines" (Chapter 3: Cybersecurity Practices)
- NERC "Security Guideline for the Electricity Sector: Protecting Sensitive Information"
- TSA "Pipeline Security Guidelines" (Chapter 6.2: Baseline and Enhanced Measures, Recordkeeping Measures)
- NIST "Cybersecurity Framework" (Appendix A: Framework Core)

To maintain consistent levels of information protection organization-wide, standards for the classification of information can be defined based on the sensitivity and criticality of the information asset, which will assist in the processing of sensitive information requests. In identifying and classifying sensitive information, owners and operators generally first follow their internal company policies and procedures and comply with all applicable regulatory requirements. To ensure classification system clarity, private sector classification guidance may state that it is a representation of private sector information classification levels and not of information classification levels used by the United States Government.

Using, processing, storing, reproducing, transmitting, and destroying classified United States Government information must be completed under the appropriate information classification and security regime and must be consistent with the appropriate laws, executive orders, directives, regulations, and authorized agency controls. Federal Government agencies should follow Federal information classification guidelines. State and local facilities should follow State and local information classification guidelines, respectively, and apply Federal information classification guidelines when handling information created or received by an agency of the Federal Government. State and local facilities should take into account applicable public records laws when implementing a State or local information classification system. Local facilities lacking information classification guidelines should develop guidelines and may use, as appropriate, the guidance included within this document.

The following represents private sector classification levels in handling and processing requests for information and does not represent an exhaustive listing of classification levels or designations across the sector. For example, some companies may label information with other designations, such as "Business Sensitive" instead of "Internal Use," or "Privileged" instead of "Confidential."

- **Public Level:** Data or information that is lawfully, properly, and regularly disclosed generally or broadly to the public that does not have restrictions. For example, the physical location of a critical asset without any designation of criticality (e.g., the address of the building housing a transmission control center).
- **Organization Level (e.g., Designated as Internal Use, Private):** Data or information regarding critical assets, key facilities, and systems maintaining the reliability and security of dam systems that may require protective measures. For example, documents that are the property of the organization and not to be further shared without permission (e.g., one-line diagrams showing critical facilities).
- **Restricted Level (e.g., Designated as Confidential, Secret):** Organization data or information regarding critical assets, key facilities, and systems maintaining the reliability and security of dam systems that may require secure restrictions and is typically not shared with other entities. For example, results of engineering studies showing system weaknesses or vulnerabilities within the electrical system.

Identifying Potentially Sensitive Information

The following questions can help to identify potentially sensitive information:

- As it relates to your company's critical assets, key facilities, or systems, does the information contain operational procedures, lists relating to critical assets and identified critical cyber assets, network topology or similar diagrams, floor plans of computing centers that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information?
- What impact on critical assets, key facilities, and the system could the information have if it inadvertently reached an unintended audience, or was used in conjunction with publicly available information?
- Does the information contain personal details of key operating personnel such as biographical data, contact information, names, addresses, or telephone numbers?
- Could someone intent on causing harm to personnel or critical assets, key facilities, and systems use the information to his or her advantage?

Source: NERC "Security Guideline for the Electricity Sector: Protecting Sensitive Information"

Regardless of the type of classification level system implemented, all information distribution should comply with stated organization policies, agency regulations, and all applicable laws. The owner of the information is responsible to appropriately classify, label, handle, and destroy information. A document containing sensitive information, but has not been designated as such, should be returned to the information owner for proper classification and designation. To ensure consistent classification and subsequent protection of information, procedures could be developed to mark, store, and transmit information.

Once information assets are identified and effectively classified, an organizational information security policy can be established to protect the various information assets.

Protect

The sensitivities associated with revealing facility-specific operational and vulnerability information are obvious and make the protection of information a critical security measure to implement. To ensure that any security-related documents are properly protected from unauthorized access, use, disclosure, disruption, modification, inspection, or destruction, information security processes are developed and documented and then implemented organization-wide. Owners and operators may comply with their respective agencies' or organization's information security policies or contact their organization's security officer for information on marking, handling, and protecting sensitive information. An important part of information security is that personnel understand their roles and responsibilities as they relate to protecting sensitive information. Baseline information security coordination and responsibility measures can be applied to information assets:

Resources for Additional Information

- "Dams Sector Security Guidelines" (Chapter 3: Cybersecurity Practices)
- "Dams Sector Protective Measures Handbook" (FOUO) (Appendix H, Sub-Section VII: Information Security)
- "Dams Sector-Specific Plan"
- TSA "Pipeline Security Guidelines" (Chapter 7: Cyber Asset Security Measures
- NIST "Cybersecurity Framework" (Appendix A: Framework Core)

- Develop a cross-functional cybersecurity team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks.
- Define information and cybersecurity roles, responsibilities, and lines of communication between the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors.
- Establish and document standards for cybersecurity controls for use in evaluating systems and services for acquisition. Encourage contractors/vendors to follow software development standards for trustworthy software throughout the development life cycle.

Information-Sharing Mechanisms

Information sharing helps to facilitate the security of all asset types—physical, cyber, personnel, and information. Successful security practices and effective resilience strategies rely on regular, timely, and accurate threat, vulnerability, and consequence information. Given the changeable nature of risk information, particularly threat information, owners and operators rely on a reliable, steady stream of information to secure the facility and various assets.

Robust information-sharing practices incorporate both the internal sharing of information, such as in facility security briefings, and the external sharing of information, such as through the Dams Sector Information Sharing Environment (ISE). The Dams Sector ISE enables trusted and vetted sector partners and stakeholders to access and share sensitive information via the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Dams Portal.

When joining the Dams Sector ISE, partners may receive DHS information-sharing products, such as the National Infrastructure Coordination Center's (NICC) Current Situation Reports or the DHS Office of Cyber and Infrastructure Analysis' Infrastructure Impact Assessment. Owners and operators can use various information-sharing mechanisms to facilitate the security of all asset types:

- **HSIN-CI:** HSIN-CI is a trusted, Internet-based information-sharing network that allows sector partners to collect and disseminate information among Federal, State, and local agencies, as well as the private sector. HSIN-CI is used to analyze relevant data and send alerts and notices, and provides a forum for vetted members to access sensitive but unclassified information relevant to sector issues.
- **HSIN-CI Dams Portal:** The Dams Portal on HSIN-CI is the primary information-sharing mechanism for the Dams Sector and enables information-sharing activities:
  - Submit suspicious activities using the Suspicious Activity Report (SAR) Tool.
  - Share sensitive information among trusted members in members-only areas, including areas for only private sector users.
  - Research Dams Sector security and protection related documents, including roadmaps, handbooks, technical guidelines, and strategic documents using the Reference Library Tool.
  - Access training products, including Dams Sector Internet-based training modules, Webinars, and other related courses through the Training Tool.
  - Host virtual presentations, review and editing of documents, and live chat (instant message) with other experts in the field using the Webinar Tool.
  - Stay up-to-date on emerging threats and incident information through the Intelligence Bulletins and Notes Tool.

Joining the Dams Sector ISE

Dams Sector community partners, stakeholders, and cross-sectors may join the Dams Sector ISE, participate in sector-wide information-sharing efforts, and access DHS information-sharing products by submitting a request to dams@hq.dhs.gov. Requests to join the Dams Sector ISE should include:

- Agency/company/organization information
- Organizational affiliation
- Supervisor information
- Basis for request
- Work email address

Resources for Additional Information

- "Dams Sector Information Sharing Resource Guide"
- Dams Sector Suspicious Activity Reporting Website
- Dams Sector Suspicious Activity Reporting Tool
- HSIN-CI Dams Portal
- "Dams Sector-Specific Plan"
- FERC "Security Program for Hydropower Projects" (Appendix C: Procedures for Reporting Suspicious Activity)

- **Executive Notification System (ENS):** The ENS is a DHS-sponsored notification system retained by the NICC and designed to send out rapid notification to members of the Dams Sector ISE. These notifications contain actionable information requiring immediate attention and careful review.
- **Other Mechanisms:**
  - The Dams Sector-Specific Agency ensures that all applicable steady-state and situational messages and alerts and warnings issued by the NICC and other critical infrastructure partners are disseminated to sector partners. Mechanisms may include HSIN, unclassified and classified e-mail, Dams Sector Threat Call, Critical Infrastructure Stakeholder Teleconference, secure teleconferences, and other mechanisms as appropriate.
  - State dam safety offices, State and major area urban fusion centers, Joint Terrorism Task Forces, and State and local law enforcement services may also be utilized to collect and share threat-related information.
  - DHS resources such as the Technical Resource for Incident Prevention (TRIPwire), Protective Security Advisor Program, and Private Sector Clearance Program are also used to share information with the Dams Sector ISE. In addition, the U.S. Cyber Emergency Response Team (US-CERT) and the Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT) provide cyber and advanced network/system threat activity analysis and disseminate timely, actionable information.

Suspicious Activity Reports

A suspicious activity report (SAR) is an official report of information pertaining to activities that may potentially be associated with pre-incident surveillance, activities exploring or targeting a critical infrastructure facility or system, or any possible violation of law or regulation that could compromise the facility or system in a manner that could cause an incident that would jeopardize life or property. A sample suspicious activity report is provided in *Appendix G* of this document.

What is Suspicious Activity?

Suspicious activity is defined as: "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity"

–ISE-SAR Functional Standard 1.5.5

Recognizing Suspicious Activity

- Maintain awareness of your environment
- Identify behaviors that are out of the ordinary or "suspicious"
- Report the activity with as much detail as possible

Communication with personnel and contractors/vendors about security concerns and suspicious activities is crucial to the security of all asset types and personnel. Owners and operators may develop a method for personnel and trusted contractors/vendors to report security-related incidents and suspicious activity through a SAR. To ensure timely and accurate information sharing, internal procedures would be established and disseminated that would include detailed instructions regarding submission, i.e., the facility representative to whom the SAR should be delivered and the proper authority to which the designee should forward the information. It is critical that any criminal activity be reported to the appropriate law enforcement authorities. It is also important to protect the rights of U.S. persons by ensuring personal information is not disseminated or disclosed to anyone who does not have the authority and need to access such information.

To help facilitate efficient information sharing and analysis of reported suspicious activity, the Dams Sector developed an Internet-based SAR tool to provide sector partners with the capability to report and retrieve information pertaining to suspicious activities. This reporting tool is accessible through the HSIN-CI Dams Portal. The online SAR Tool is not intended to replace, supersede, or bypass existing organizational reporting mechanisms or regulatory reporting requirements, but rather to enhance them by providing a broader approach to reporting suspicious activity.

There is more than one way to report a SAR, although all criminal activity or security incidents should be reported to the appropriate law enforcement authorities. The following information outlines a sample pathway for reporting SARs:

- Report criminal activity or security incidents requiring an immediate security response to the local law enforcement agency (911). This step is imperative for all such incidents, regardless of other possible variations to the reporting pathway.
- Obtain and record as much identifying information as possible.

- Complete a SAR.
- Ensure reporting activities are in accordance with regulatory requirements and consistent with organization policies. The SAR should be forwarded per organization procedures and policy.

Submit relevant suspicious activity information to the HSIN-CI Dams Portal for sector situational awareness and further analysis. Personally identifiable information, which is defined as any information about an individual that can be used to distinguish or trace an individual's identity (e.g., name, social security number, date of birth, mother's maiden name, biometric records) should not be provided.

Figure 6. Sample pathway for reporting suspicious activity

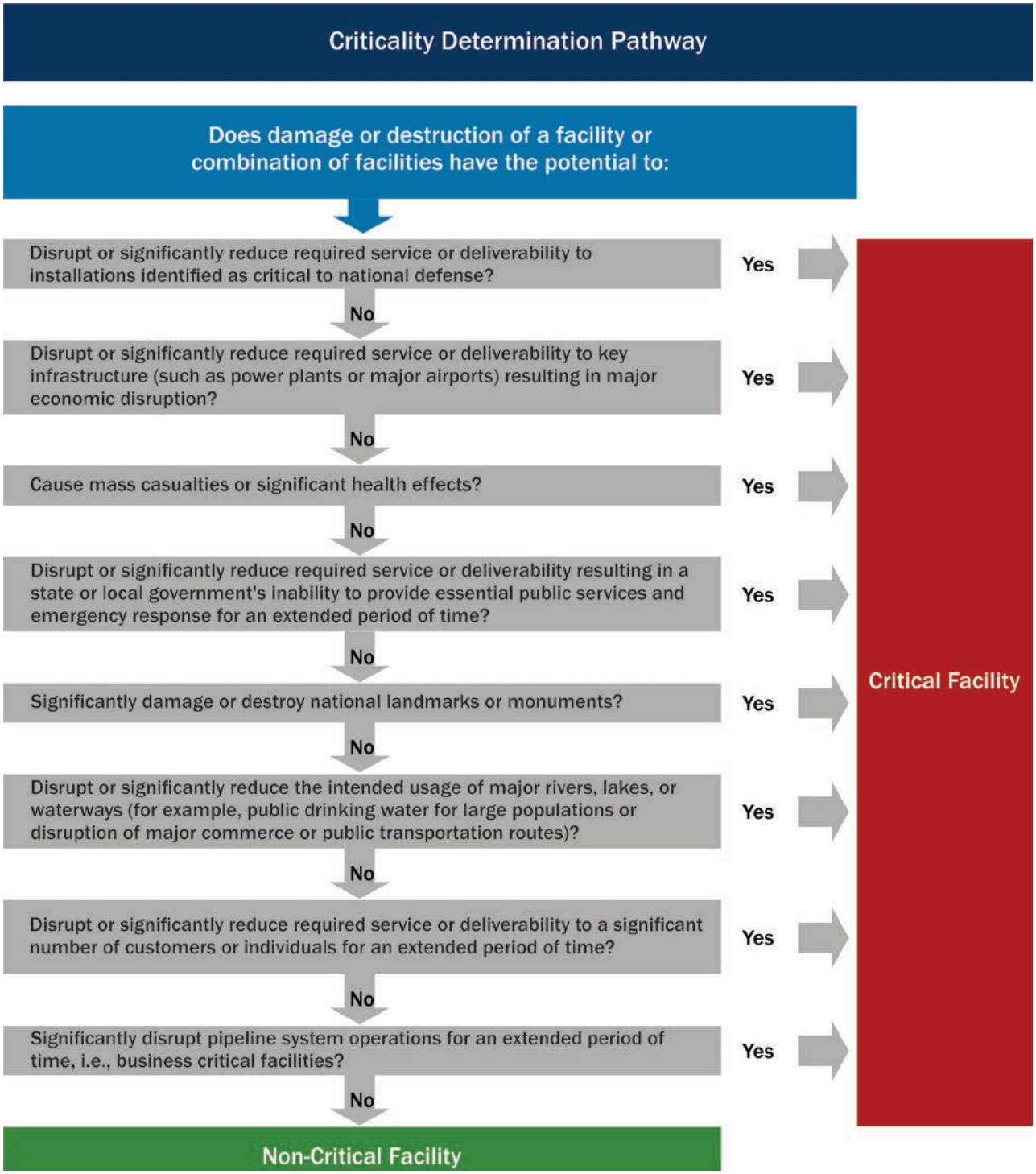
Appendix A: Key Terms and Acronyms

ASCE	American Society of Civil Engineers
C2M2	Cybersecurity Capability Maturity Model
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability assessment methodology
CFR	U.S. Code of Federal Regulations
CIKR	Critical Infrastructure and Key Resources
CIPR	Critical Infrastructure Protection and Resilience
CIP	Critical Infrastructure Protection
CRM-D	Common Risk Model for Dams
CRR	Cyber Resilience Review
CSET	Cyber Security Evaluation Tool
CSIRTs	Computer security incident response team
CTS	Consequence-Based Top Screen Methodology
DAMSVR	Dam Assessment Matrix Security Vulnerability Risk
DHS	U. S. Department of Homeland Security
EAPs	Emergency action plan
ENS	Executive Notification System
EO	Executive Order
EPA	U.S. Environmental Protection Agency
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FOUO	For Official Use Only

HSEEP	Homeland Security Exercise and Evaluation Program
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
ICS	Incident Command System (as a component of the National Incident Management System)
ICS-CERT	Industrial Control Systems – Cyber Emergency Response Team
ISE	Information-sharing environment
IT	Information technology
NERC	North American Electric Reliability Corporation
NICC	National Infrastructure Coordinating Center
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NTAS	National Terrorism Advisory System
RIDM	Risk-Informed Decision Making
RAM-D	Risk Assessment Methodology for Dams
SAR	Suspicious activity report
SCADA	Supervisory control and data acquisition
SSI	Sensitive security information
SVA	Security vulnerability assessment
SWAT	Special Weapons and Tactics
TRIPwire	Technical Resource for Incident Prevention
TSA	Transportation Security Administration
USACE	U.S. Army Corps of Engineers
US-CERT	U.S. Cyber Emergency Response Team
VSAT	Vulnerability Self Assessment Tool

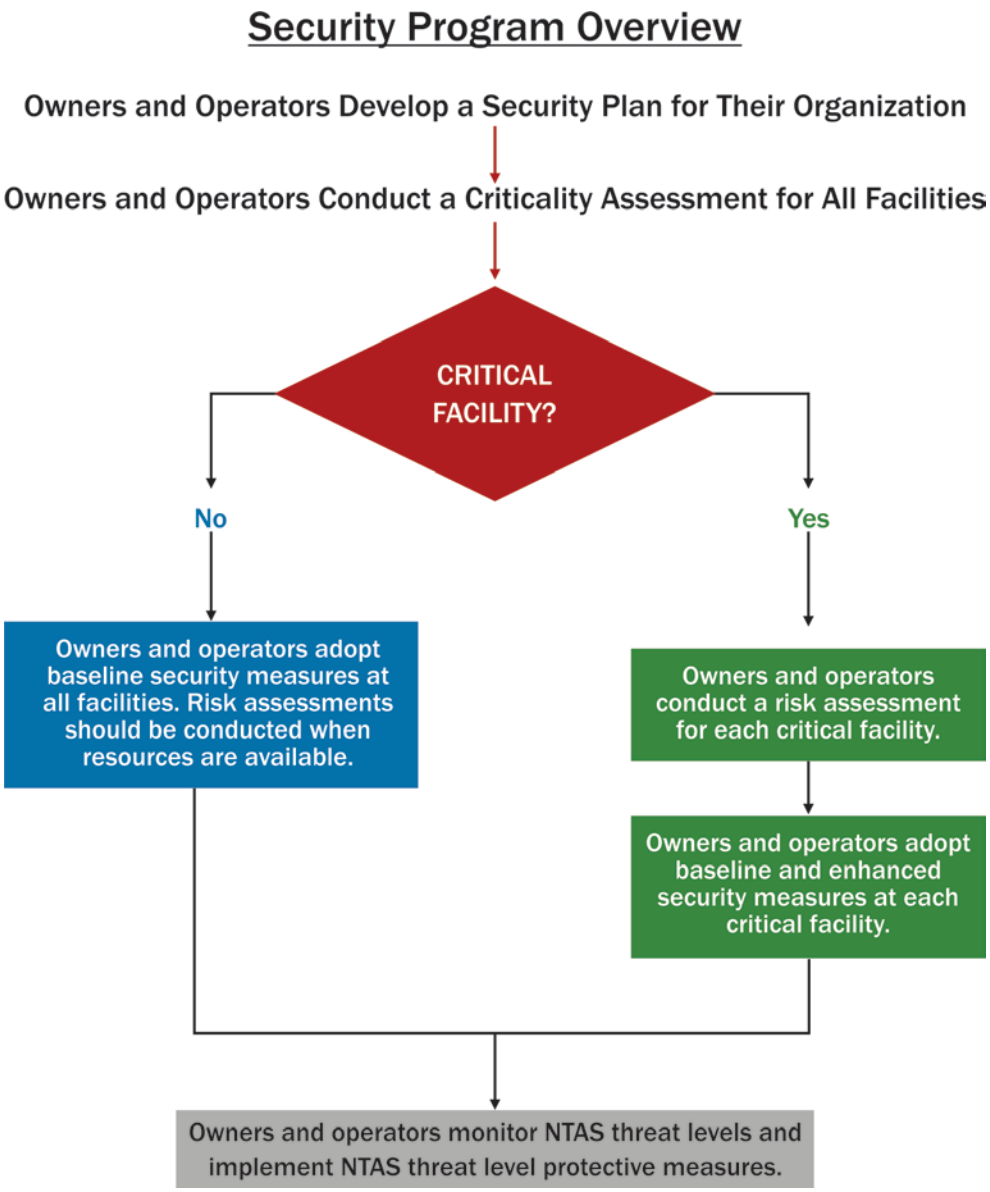
Appendix B: TSA Criticality Determination Pathway

The following criticality determination pathway is amended from the TSA "Pipeline Security Guidelines" (2011). Please see pages 9–10 of the TSA document for additional information.



Appendix C: TSA Corporate Security Program Overview

The following graphical overview of a corporate security program is amended from the TSA "Pipeline Security Guidelines" (2011). Please see pages 3–4 of the TSA document for additional information.



Appendix D: TSA Baseline and Enhanced Security Measures

The following chart of baseline security measures and enhanced security measures is amended from the TSA "Pipeline Security Guidelines" (2011). Please see pages 11–15 of the TSA document for additional information.

	Baseline Security Measures	Enhanced Security Measures
Physical Security and Access Controls	**Barriers**	
	Maintain fences, if used, without gaps around gates or underneath the fence line. Ensure that there is a clear zone for several feet on either side of the fence, free of obstructions, vegetation, or objects that could be used to scale the fence.	Create a security perimeter that deters unauthorized vehicles and persons from entering the facility perimeter or critical assets by installing and maintaining barriers (for example, fences, bollards, jersey barriers, or equivalent).
	Employ measures to deter unauthorized vehicles and persons from penetrating facility perimeters.	
	Access Controls	
	Employ measures to deter unauthorized persons from gaining access to a facility and restricted areas within a facility.	Implement procedures (such as manual and electronic sign in/out) for controlling access to the facility and restricted buildings or areas within the facility (e.g., visitors, contractors, or employees).
	Close and secure doors, gates, or entrances when not in use.	Monitor and escort visitors at critical facilities.
	Post "No Trespassing" or "Authorized Personnel Only" signs at intervals that are visible from any point of potential entry.	
	Gates	
		Install and maintain gates of a quality equivalent to the barrier to which they are attached.
	Locks and Key Control	
		Establish and document key control procedures for key tracking, issuance, collection, and loss. Use patent keys to prevent unauthorized duplication. Conduct key inventories every 24 months.
	Facility Lighting	
		Provide sufficient illumination for human or technological recognition of intrusion.
	Intrusion Detection and Monitoring	
		Equip critical facilities or critical areas within a facility with 24/7 monitoring capability to detect and assess unauthorized access.
Personnel Security	**Personnel Identification and Badging**	
	Develop identification and badging policies and procedures for employees and onsite personnel who have access to secure areas or sensitive information. These policies should address: • Lost or stolen identifications cards or badges • Termination • Temporary badges	Ensure that company or vendor identification is visibly displayed by employees and contractors while onsite.
		Ensure employee and contractor identification cards or badges are secure from tampering and contain the individual's photograph and name.

	Baseline Security Measures	Enhanced Security Measures
	Background Investigation	
	Establish policies and procedures for applicant pre-employment screening and behavior criteria for disqualification of applicants and employees.	Conduct pre-employment background investigations of applicants for positions that are: • Authorized regular unescorted access to control systems or sensitive areas • Authorized access to sensitive information • Assigned to security roles • Assigned to work at or granted access rights to critical facilities At a minimum, investigations should: • Verify and validate identity • Check criminal history* • Verify and validate legal authorization to work *NOTE: Operators should consider using the federally established list of disqualifying crimes applicable to transportation workers at ports (see 49 CFR 1572.103) to assess the suitability of their employees and contractors for these positions.
		Verify that contractors have background investigation policies and procedures at least as rigorous as the pipeline operator's.
		Conduct recurring background investigations on a regular basis, not to exceed 10 years, for employees occupying security positions or who have access to sensitive information or areas.
Equipment Maintenance and Testing	**Equipment Maintenance and Testing**	
	Develop and implement a maintenance program to ensure security systems are in good working order.	Verify the proper operation and/or condition of all security equipment on a quarterly basis.
	Identify and respond to security equipment malfunctions or failures in a timely manner.	Conduct an annual inventory of security equipment.
		Provide alternate power sources (for example, generators or battery back-up) or equivalent equipment to minimize interruption of security equipment operation.
Design and Construction	**Design and Construction**	
	Integrate security measures during the design, construction, or renovation of a facility.	Update the facility security vulnerability assessment (SVA) within 12 months following significant modifications.
Communication	**Communication**	
	Develop internal and external notification requirements and procedures for security events.	Ensure primary and alternate communication capabilities exist for internal and external reporting of all appropriate security events and information.
	Document and periodically update contact (who) and communication (how) information for Federal, State, and local homeland security/law enforcement agencies.	Establish a defined process for receiving, handling, disseminating, and storing security and threat information.

	Baseline Security Measures	Enhanced Security Measures
Personnel Training		
Personnel Training	Provide security awareness briefings for all employees and contractors with unescorted access upon hire and every two (2) years thereafter.	Provide security training, including incident response training, to all full-time, part-time, and contract employees assigned security duties upon hire and annually thereafter.
Personnel Training	Document and maintain records for all security training in accordance with company record retention policy.	
Exercises and Drills		
Exercises and Drills	Conduct periodic security drills or exercises, including unannounced tests of security and incident plans. These can be conducted in conjunction with other required drills or exercises.	Conduct or participate in an annual security drill or exercise.
Exercises and Drills	Develop and implement a written post-exercise report assessing security exercises and documenting corrective actions.	
Security Incident Procedures		
Security Incident Procedures	Implement procedures for responding to security incidents or emergencies and to NTAS threat alerts. These procedures should include the appropriate reporting requirements.	
Recordkeeping		
Recordkeeping	Develop and document recordkeeping policies and procedures for security information. Protection of Sensitive Security Information (SSI) in accordance with the provisions of 49 CFR part 1520 should be specifically addressed.	
Recordkeeping	At a minimum, the following documents, as appropriate, should be retained until superseded or replaced: • Corporate security plan • Criticality assessment(s) • Training records • Exercise reports • Incident response plan(s) • Security testing and audits • Security equipment maintenance and testing records Make security information records available to TSA upon request.	In addition to the documents specified for non-critical facilities, the following documents, applicable to critical facilities, should be retained until superseded or replaced: • SVA(s) • Site-specific measures Make security information records available to TSA upon request.

Appendix E: Baseline and Enhanced Cybersecurity Measures

The following chart of baseline and enhanced cybersecurity measures is amended from the FERC "Security Program for Hydropower Projects." Please see pages 43–45 of the FERC document for additional information.

Baseline Cybersecurity Measures: The baseline measures should be applied to all cyber assets or cyber systems	
General Cybersecurity	Provide physical security and access controls to cyber assets. Ref: NIST SP 800-82 Section 6.2.1.
	Monitor and periodically review (not to exceed 18 months) network connections, including remote and third-party connections.
	Evaluate and reassess the role of wireless networking for risk before implementation. Ref: NIST SP 800-153.
	Review and reassess all cybersecurity procedures annually. Update procedures as necessary.
	Review and reassess cyber asset criticality periodically, (not to exceed 12 months). In addition, criticality should be determined as all new cyber assets are added to the environment.
Information Security Coordination Responsibilities	Develop a cross-functional cybersecurity team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks. Ref: NIST SP 800-82 Section 4.2.
	Define information and cybersecurity roles, responsibilities, and lines of communication among the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors.
	Establish and document standards for cybersecurity controls for use in evaluating systems and services for acquisition. Encourage vendors to follow software development standards for trustworthy software throughout the development lifecycle. Ref: NIST SP 800-82 Section 6.2.15, NIST SP 800-23, NIST SP 800-36, NIST SP 800-64, and DHS Cyber Security Procurement Language for Control Systems.
System Lifecycle	Incorporate security into cyber system design and operation, whether designing a new system or modifying an existing system. Secure design and operation of the SCADA control system architecture is critical for the creation of a sustainable and reliable system. Mitigate any security deficiencies found in control system hardware and software. Ref: NIST SP 800-27, NIST SP 800-64, and NIST SP 800-70.
	Establish and document policies, standards, and procedures for assessing and maintaining system status and configuration information, for tracking changes made to control systems network, and for patching and upgrading operating systems and applications. Ref: NIST SP 800-40.
	Establish and document policies, standards, and procedures for the secure disposal of equipment and associated media. Ref: NIST SP 800-82 Section 6.2.10 and NIST SP 800-88.
System Restoration & Recovery	Plan and prepare for the restoration and recovery of control systems in a timely manner as specified in the facility's recovery procedures. Ref: NIST SP 800-82 Section 5.13, NIST SP 800-82 Section 6.2.6, NIST SP 800-34, and NIST SP 800-100.
	Review the restoration and recovery plan for control systems including annual testing of plan.
Intrusion Detection & Response	Establish policies, standards, and procedures for cyber-intrusion monitoring, detection, incident handling, and reporting. Ref: NIST SP 800-61, NIST SP 800-82 Section 5.1, NIST SP 800-82 Section 5.16, NIST SP 800-83, NIST SP 800-94, and NIST SP 800-82 Appendix E.
Training	Provide training in information security awareness, on an annual basis or as necessitated by changes in the control system, for all users of control systems before permitting access to the control systems. Individuals with significant control systems security roles should have advanced training specific to their roles. Ref: NIST SP 800-16, NIST SP 800-82 Section 6.2.2, and NIST SP 800-50.

Baseline Cybersecurity Measures: The baseline measures should be applied to all cyber assets or cyber systems	
Access Control & Functional Segregation	Segregate and protect the control systems network from the business network and the Internet through the use of firewalls and other protections. This applies both to wired and wireless networks. Ref: NIST SP 800-82 Sections 5.2, 5.3, 5.5, and 5.6.
	Use control systems servers and desktop computers only for approved control system activities.
	Establish and enforce access control policies for local and remote users, guests, and customers. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections to control networks. Ref: NIST SP 800-82 Section 6.2.1 and NIST SP 800-82 Section 6.2.7.

Enhanced Cybersecurity Measures In addition to baseline measures, to be applied to all cyber assets or systems classified as critical	
Access Control	Restrict physical and logical access to control systems and control networks through the use of an appropriate combination of locked facilities, passwords, secured communication gateways, access control lists, authenticators, separation of duties practices, least privilege practices, and/or other secure access mechanisms and practices. Ref: NIST SP 800-82 Section 6.3.2.
	Conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Evaluate the need for enhanced networking control technologies for wireless networks prior to implementation. Ref: NIST SP 800-115 Section 6 and NIST SP 800-82 Section 3.
Vulnerability Assessment	Conduct periodic vulnerability assessments of the control system security, including as appropriate in a non-production environment, not to exceed 12 months. Ref: NIST SP 800-40, NIST SP 800-82 Section 6.2.14, NIST SP 800-115, and NIST SP 800-82 Appendix E.

Appendix F: Sample Security Plan Outline

The following is a sample outline of a security plan to assist owners or operators in developing a security plan for their specific sites or projects. Security plan templates are located in Appendix H of the "Dams Sector Protective Measures Handbook" (FOUO), on the HSIN-CI Dams Portal, or upon request from dams@hq.dhs.gov.

1. INTRODUCTION, PURPOSE, AND SCOPE
2. APPLICABILITY, DEFINITIONS, AND RESPONSIBILITIES
    - 2.1 Applicability
    - 2.2 Definitions
    - 2.3 Designated Personnel Responsibilities
        - 2.3.1 Incident Commander
        - 2.3.2 Security Coordinator
        - 2.3.3 Risk Coordinator
        - 2.3.4 Corporate Communications Coordinator
        - 2.3.5 Other positions as required
3. SITE DESCRIPTION
4. OPERATIONAL PROCEDURES
    - 4.1 General Security Guidelines
    - 4.2 Security Personnel
    - 4.3 General Access Requirements
    - 4.4 Prohibited Items
    - 4.5 Weapons
    - 4.6 Key Control
    - 4.7 Information Protection
5. RESTRICTED AREAS
6. CRITICAL ASSET LIST AND DESCRIPTIONS
7. PHYSICAL SECURITY FOR CRITICAL ASSETS
    - 7.1 Purpose
    - 7.2 Responsibilities
    - 7.3 Physical Security Descriptions, Layout, and Inventory
    - 7.4 Physical Security Standards and Administration
    - 7.5 Access Controls
    - 7.6 Reception Lobbies and Other Entry Points

7.7 Electronic Access Controls

7.8 Securing Computers

7.9 Securing Desktop Computers

7.10 Securing Laptop Computers

7.11 Protection of Sensitive Information

7.12 Protection of Sensitive Data

7.13 Use of Courier Services to Ship Sensitive Information

7.14 Protection of Security System Servers

7.15 Security Check Process

7.16 Access Control, Intrusion, and Closed-Circuit Television System Maintenance

7.17 Key Control Program

7.18 Access Card Maintenance

7.19 Closed-Circuit Television System Components and Performance

7.20 Requests to View and/or Copy Video Activity

7.21 Fencing, Barriers, and Gates

7.22 Intruder Alarm Systems

7.23 Vehicles and Equipment

7.24 Security Personnel and Training

7.25 Exceptions to the Plan (if any)

8. INFORMATION TECHNOLOGY
9. CYBERSECURITY AND SCADA SYSTEMS
10. COMMUNICATIONS SYSTEMS
11. SECURITY SYSTEMS MAINTENANCE AND TESTING
12. THREAT LEVEL PLANNING

    12.1 General Conditions

    12.2 Elevated Threat Conditions

    12.3 Imminent Threat Conditions

13. BOMB THREATS AND RESPONSE
14. CIVIL DISTURBANCES
15. WORKPLACE VIOLENCE AND ACTIVE SHOOTER RESPONSE
16. REPORTING SECURITY INCIDENTS
17. INVESTIGATIONS
18. EMERGENCY PREPAREDNESS AND RECOVERY
19. TEMPORARY FACILITY CLOSURE PROCEDURES
20. SECURITY PLAN REVIEW, MAINTENANCE, AND SCHEDULES

Appendix G: Sample Suspicious Activity Report

The following sample suspicious activity reporting form is amended from Appendix C of the FERC "Security Program for Hydropower Projects."

SAMPLE SUSPICIOUS ACTIVITY REPORTING FORM
(Mark as "Privileged – Security Sensitive Material")

Incident Entered By:_____

Originating Agency:_____

Originators Email Address:_____

Incident Title: (The incident title should be a short narrative similar to a news article headline that will summarize the activity)

_____

_____

_____

_____

Agency Report #/ID: _____

Reporting Officer:_____

Date of Incident:_____

Time Incident Observed: _____

Time Zone Incident Observed: _____

Incident Type: (For incident type, chose one of the Categories of Suspicious Activity that are listed in Appendix C of FERC "Security Program for Hydropower Projects")

_____

Incident Sub-Type: (For example, if the incident type is Surveillance, then the Sub-type could be photography or video)

_____

Incident Summary: (The incident summary is the body of your report. Provide as much detail as possible here about the incident)

Action Taken: (List any coordination with law enforcement or other actions taken)

Incident Location:

Name of Location:

Type of Location:

Address of Location:

Submit any applicable attachments with this report. Depending on the nature of the SAR, terrorism-related and other cyber or criminal threat information included within may be submitted to eGuardian for investigation by the U.S. Federal Bureau of Investigation (FBI). eGuardian is a database developed and operated by the FBI and is limited to users who have a need to know and who undergo a strict vetting process. SAR information will not be further distributed without the express consent of the originating agency. A complete report greatly assists the investigation process. In particular, information such as incident location, type of incident, and any other identifying information can greatly increase the FBI's and/or other law enforcement entities' chances of conducting a complete investigation. It is possible that the FBI may require additional information; for this reason, the point of contact identified on the SAR may be contacted.

Appendix H: Source Documents and Websites

Chapter 1: Critical Asset Identification

Dams Sector Consequence-Based Top Screen (CTS) Methodology. http://www.dhs.gov/publication/dams-Consequence-Based-top-screen-fs (accessed October 26, 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

FERC Dam Assessment Matrix for Security and Vulnerability Risk (DAMSVR), https://www.ferc.gov/industries/hydropower/safety/guidelines/security/damsvr.asp (accessed October 26, 2015).

FERC: Security Program for Hydropower Projects, http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf (accessed October 26, 2015).

Interagency Security Committee: Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, http://www.dhs.gov/publication/isc-risk-management-process (accessed October 26, 2015).

NERC: Cyber Security – Critical Cyber Asset Identification Standard, http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-3&title=Cyber Security - Critical Cyber Asset Identification&jurisdiction=null (accessed October 26, 2015).

NERC: Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets, http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf (accessed October 26, 2015).

Transportation Security Administration (TSA): Pipeline Security Guidelines. Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Chapter 2: Physical Security Practices

American Society of Civil Engineers (ASCE): Guidelines for the Physical Security of Water Utilities and of Wastewater/Stormwater Utilities, http://www.asce.org/templates/publications-book-detail.aspx?id=8073 (accessed October 26, 2015).

ASIS International: Facilities Physical Security Measures Guideline, https://www.asisonline.org/Standards-Guidelines/Guidelines/Published/Pages/Facilities-Physical-Security-Measures-Guideline.aspx (accessed October 26, 2015).

Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability (CARVER) Assessment Methodology. Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Consequence-Based Top Screen (CTS) Methodology, http://www.dhs.gov/publication/dams-Consequence-Based-top-screen-fs (accessed October 26, 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Crisis Management Handbook. Accessible on the HSIN-CI Dams Portal: http://www.dhs.gov/homeland-security-information-network-dams-portal (accessed October 26, 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Emergency Preparedness Guidelines for Levees, http://www.usace.army.mil/Portals/2/docs/civilworks/levee/EP_guidforlevees.pdf (accessed October 26, 2015).

Dams Sector Estimating Economic Consequences for Dam Failure Scenarios, https://www.damsafety.org/media/documents/owner%20documents/Dam%20Security/Dams%20Sector%20-%20Consequence%20Estimation%20-%20Economic%20Consequences.pdf (accessed October 26, 2015).

Dams Sector Estimating Loss of Life for Dams Failure Scenarios, http://www.damsafety.org/media/Documents2/security/files/DamsSectorConsequenceEstimation_LossOfLife.pdf (accessed October 26, 2015).

Dams Sector Protective Measures Handbook (FOUO). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.Dams Sector Security Awareness Guide, http://www.dhs.gov/publication/dams-sector-security-awareness-guide (accessed October 26, 2015).

Dams Sector Security Awareness Guide for Levees, http://www.dhs.gov/publication/dams-security-awareness-guide-levees (accessed October 26, 2015).

Dams Sector-Specific Plan. http://www.dhs.gov/publication/dams-sector-specific-plan (accessed October 26, 2015).

DHS Risk Lexicon, http://www.dhs.gov/dhs-risk-lexicon (accessed October 26, 2015).

DHS Risk Management for the Water Sector Training, https://share.dhs.gov/riskmanagementwatersectortraining/(accessed October 26, 2015).

EPA Vulnerability Self Assessment Tool (VSAT), http://water.epa.gov/infrastructure/watersecurity/techtools/vsat.cfm (accessed October 26, 2015).

FEMA Risk Prioritization Tool for Dams, https://www.fema.gov/media-library/assets/documents/13523?id=3296 (accessed October 26, 2015).

FERC Dam Assessment Matrix for Security and Vulnerability Risk (DAMSVR) https://www.ferc.gov/industries/hydropower/safety/guidelines/security/damsvr.asp (accessed October 26, 2015).

FERC Risk-Informed Decision Making (RIDM), http://www.ferc.gov/industries/hydropower/safety/initiatives/risk-informed-decision-making.asp (accessed October 26, 2015).

FERC: Security Program for Hydropower Projects, http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf (accessed October 26, 2015).

NERC: Security Guideline for the Electricity Sub-sector: Physical Security Response http://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/Electricity%20Sector%20Physical%20Security%20Guideline%20(Approved%20by%20CIPC%20-%20October%2028,%202013).pdf (accessed October 26, 2015).

National Terrorism Advisory System (NTAS), http://www.dhs.gov/alerts (accessed October 26, 2015).

Risk Assessment Methodology for Dams (RAM-D). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

U.S. Army Corps of Engineers (USACE) Common Risk Model for Dams (CRM-D) Risk Assessment Methodology Contact the USACE Critical Infrastructure Protection & Resilience (CIPR) Program at CIPR@usace.army.mil.

Chapter 3: Cybersecurity Practices

Dams Sector Crisis Management Handbook. Accessible on the HSIN-CI Dams Portal: http://www.dhs.gov/homeland-security-information-network-dams-portal (accessed October 28, 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Cybersecurity Capability Maturity Model (C2M2) (to be released in 2015). Contact the Dams Sector-Specific Agency at: dams@hq.dhs.gov.

Dams Sector: NIST Cybersecurity Framework Implementation Guide. Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Roadmap to Secure Control Systems, http://www.damsafety.org/media/Documents2/security/files/DamsSectorRoadmapToSecureControlSystems.pdf (accessed October 28, 2015).

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity (accessed October 28, 2015).

FERC: Security Program for Hydropower Projects, http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf (accessed October 28, 2015).

ICS-CERT Cyber Security Evaluation Tool (CD, onsite training, guidance), https://ics-cert.us-cert.gov/Assessments (accessed October 28, 2015). Contact CSET@hq.dhs.gov.

NERC: CIP Standards – Cyber Security (CIP-002-3 – 009-3), http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed October 28, 2015).

NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/ (accessed October 28, 2015).

US-CERT Cyber Resilience Review (onsite assessment, self-assessment resources), https://www.us-cert.gov/ccubedvp/self-service-crr#Downloadable%20Resources (accessed October 28, 2015). Contact CSE@hq.dhs.gov.

Chapter 4: Personnel Security Practices

American Society of Civil Engineers (ASCE): Guidelines for the Physical Security of Water Utilities and of Wastewater/Stormwater Utilities, http://www.asce.org/templates/publications-book-detail.aspx?id=8073 (accessed October 28, 2015).

Dams Sector Crisis Management Handbook. Accessible on the HSIN-CI Dams Portal: http://www.dhs.gov/homeland-security-information-network-dams-portal (accessed October 28, 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Personnel Screening Guide for Owners and Operators, http://www.dhs.gov/publication/personnel-screening-guide-owners-and-operators (accessed October 28, 2015). Dams Sector Protective Measures Handbook (FOUO). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Security Awareness Handbook (FOUO). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector-Specific Plan, http://www.dhs.gov/publication/dams-sector-specific-plan (accessed October 28, 2015).

Dams Sector Training Schedule (and how to sign up) http://www.dhs.gov/dams-sector-training (accessed October 28, 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

FEMA: Federal Guidelines for Emergency Action Planning for Dams, https://www.fema.gov/media-library/assets/documents/3357 (accessed October 28, 2015).

FERC: Security Program for Hydropower Projects, http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf (accessed October 28, 2015).

DHS Homeland Security Exercise and Evaluation Program, http://www.fema.gov/media-library/assets/documents/32326 (accessed October 28, 2015).

National Incident Management System and Incident Command System Website, https://www.fema.gov/national-incident-management-system (accessed October 28, 2015).

Chapter 5: Information Security Practices

Dams Sector Cybersecurity Capability Maturity Model (C2M2) (to be released in 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Information Sharing Resource Guide. Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector: NIST Cybersecurity Framework Implementation Guide. Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Protective Measures Handbook (FOUO). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector-Specific Plan, http://www.dhs.gov/publication/dams-sector-specific-plan (accessed October 28, 2015) (accessed October 28, 2015).

Dams Sector Suspicious Activity Reporting Tool. Accessible on the HSIN-CI Dams Portal: http://www.dhs.gov/homeland-security-information-network-dams-portal (accessed October 28, 2015). Contact the Sector-Specific Agency at dams@hq.dhs.gov.

Dams Sector Suspicious Activity Reporting Website, http://www.dhs.gov/dams-sector-suspicious-activity-reporting (accessed October 28, 2015).

FERC: Security Program for Hydropower Projects, http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf (accessed October 28, 2015).

HSIN-CI Dams Portal, http://www.dhs.gov/homeland-security-information-network-dams-portal (accessed October 28, 2015). Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

ICS-CERT Cyber Security Evaluation Tool (CD, onsite training, guidance), https://ics-cert.us-cert.gov/Assessments (accessed October 28, 2015). Contact CSET@hq.dhs.gov.

NERC Security Guideline for the Electricity Sector: Protecting Sensitive Information, http://www.nerc.com/comm/CIPC/Protecting%20Sensitive%20Information%20Guideline%20Task1/Protecting%20Sensitive%20Information%20Guideline%20(PSIGTF).pdf (accessed October 28, 2015).

NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/ (accessed October 28, 2015).

Transportation Security Administration (TSA): Pipeline Security Guidelines. Contact the Dams Sector-Specific Agency at dams@hq.dhs.gov.

US-CERT Cyber Resilience Review (onsite assessment, self-assessment resources), https://www.us-cert.gov/ccubedvp/self-service-crr (accessed October 28, 2015). Contact CSE@hq.dhs.gov.

Homeland
Security