IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Dams Sector Security Awareness and Protective Measures

APRIL 2021

OVERVIEW

Dams, levees, and related facilities are a vital part of the Nation's infrastructure, providing a wide range of economic, environmental, and social benefits through the delivery of critical water retention and control services. While failures of Dams Sector facilities do not happen often, failures are high consequence events that can result in severe economic losses, loss of life, and reduced public confidence in industry and the government's ability to provide essential services. Dam owners and operators can reduce consequences and enhance the overall resilience of their facilities by increasing awareness of risks to the facility and taking action to reduce the risk, including by implementing protective measures.

The Cybersecurity and Infrastructure Agency, as the Sector Risk Management Agency for the Dams Sector, collaborated with sector partners to develop materials to help owners and operators enhance their security posture. The following publications and web-based independent study (IS) training courses are available on the Homeland Security Information Network—Critical Infrastructure (HSIN-CI) Dams Portal. For access to the Dams Portal, email DamsPortal@hq.dhs.gov.

- ***Dams Sector Security Awareness Handbook (FOUO)*:** Helps owners and operators to identify security concerns, coordinate response, and establish partnerships with law enforcement and first responders.
- **Dams Sector—Security Awareness (IS-871a) (FOUO):** Describes common vulnerabilities, potential indicators of threats, surveillance detection methods, and reporting of incidents and suspicious activities.
- ***Dams Sector Protective Measures Handbook (FOUO)*:** Helps owners and operators to select protective measures and includes recommendations for developing site security plans.
- **Dams Sector—Protective Measures (IS-872a) (FOUO):** Introduces protective measures concepts and describes the importance of these measures as components of an overall risk management program.
- **Surveillance and Suspicious Activities Indicators Guide for Dams and Levees:** Highlights indicators of surveillance and suspicious activity, methods for reporting suspicious activity, and other actions to take to counter surveillance and suspicious activity.

This fact sheet introduces foundational concepts included in the publications and courses. For additional information, refer to the materials listed above or contact the Dams Sector Management Team at DamsSector@cisa.dhs.gov.

SECURITY AWARENESS

Security awareness is the foundation upon which effective security programs are based. By implementing the following security awareness concepts, owners and operators can recognize security problems and respond accordingly to protect the facility and its workers and ensure continued delivery of the dam project's benefits:

- **Understand vulnerabilites:** Security vulnerabilities depend on the type of asset, the quality of construction and maintenance, and the type of control systems used. Sources of vulnerabilities include exploitation by an adversary of a condition or situation at a particular site, an interdependency due to the relationship between two or more sites, or a dependency due to operations being reliant on another site or asset.
- **Recognize indicators of threat activity:** In targeting critical infrastructure, potential adversaries can employ a wide range of weapons, tools, and tactics, including the use of explosives or a cyber-attack. Indicators of potential threat activity—including unusual or odd behavior of employees or visitors, unattended objects, or unexplained equipment failures—may be discovered through observation and reported as suspicious.

- **Report suspicious activity:** Suspicious activity reporting is the official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. Timely reporting helps local authorities act quickly to identify and mitigate against potential threats.

RISK REDUCTION STRATEGIES

Risk is defined as a function of three parameters including threat, vulnerability, and consequence. An effective protective program incorporates a well thought-out and coordinated plan of action to deter, detect, delay, assess, and respond to attacks on assets, as well as to respond to, mitigate, and recover from damage inflicted by such attacks. The objectives are to limit consequences and reduce the value of such attacks and do so cost effectively. Risk assessment results and asset-specific constraints (e.g., funding, physical characteristics, or operational considerations) will usually dictate which strategies or combination of strategies will be most appropriate. Several types of risk reduction strategies might be used, alone or in combination, to provide the desired outcomes, such as:

- **Deterrence:** Alter the adversary's perception about carrying out a successful attack.
- **Physical security:** Implement a comprehensive plan inclusive of detection, assessment, delay, and response.
- **Operational measures:** Modify operations to reduce the consequences of a successful attack.
- **Resilience:** Incorporate measures to make dam features more resilient to damage.
- **Consequence mitigation:** Take action, such as through evacuation, to reduce the effects of an attack.
- **Rapid recovery:** Take action to reestablish a dam's function after an attack.

POTENTIAL PROTECTIVE MEASURES

Protective measures can include equipment, personnel, training, and procedures designed to protect a facility against threats and to mitigate the effects of an attack or criminal activity. Decisions about which protective measures to implement are based on the owner or operator's knowledge of the history of the asset and understanding of threats, completed risk assessments, and a determination about the desired level of protection to achieve risk reduction outcomes. The following list describes potential types of protective measures:

- Instal fencing, gates, or other barriers to restrict access to the asset or support facilities.
- Limit access to critical facilities or features to authorized persons through measures such as unique or restricted keying systems, remote smart locks, or access card systems.
- Post signs in non-public areas to warn persons they are trespassing.
- Mark tools and maintain an accurate inventory of generators, power tools, and other valuable equipment to aid in their recovery if stolen.
- Ensure that metal products such as copper or aluminum are secured at night and marked to help identify them if stolen. A unique color spray paint, as well as marking and branding of wire reels may help.
- Instal door alarms or other systems to monitor entry into critical buildings or areas.
- Implement access control measures to identify and process all personnel, visitors, and vehicles (e.g., identification cards, uniforms, marked vehicles, and visitor passes).
- Install closed circuit television (CCTV) systems to provide surveillance capability of a protected facility.
- Integrate alarm, CCTV, and other security systems that report to a staffed facility or a contracted alarm station for incident assessment and dispatch of organization or law enforcement personnel as needed.
- Place barriers to delay or stop vehicles, particularly in areas where only authorized vehicles are allowed.
- Light critical areas to deter trespassers and facilitate observation at night. As an alternative, install lighting that is activated by motion detection, which also provides a deterrent effect.
- Create a security awareness program, in collaboration with local law enforcement, to advise neighbors and employees of the types of problems being experienced and how to report suspicious activities.