CISA
CYBER+INFRASTRUCTURE

Dams Sector Landscape

AUGUST 2019

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Contents

Executive Summary

The Dams Sector provides critical water retention, delivery, and control services that support multiple critical infrastructure sectors in the United States. These services include hydroelectric power generation, municipal and industrial water supplies, agricultural irrigation, sediment and flood control, river navigation for inland bulk shipping, industrial waste management, and recreation. Assets in the sector include dam projects, hydropower plants, navigation locks, levees, dikes, hurricane barriers, mine tailings, and other industrial waste impoundments. Dams Sector assets irrigate at least 10 percent of U.S. cropland, help protect more than 43 percent of the U.S. population from flooding, and generate about 60 percent of electricity in the Pacific Northwest.[1] A large and diverse set of public and private entities own and operate Dams Sector facilities under highly distributed regulatory oversight from federal, state, and local entities.

A number of factors may affect the critical infrastructure security and resilience posture of the Dams Sector. These factors, which influence the current operating environment and associated decision-making processes, stem from environmental, technological, human, and physical causes. Complete or partial dam failure could result in sudden downstream flooding that causes casualties; major environmental destruction and property damage; and cascading disruptions to the Energy, Transportation Systems, Communications, and Water and Wastewater Systems Sectors, among others. A dam or levee breach or overtopping could flood nearby communities, threaten drinking water supplies, and cause major agriculture damage. Inoperable navigation locks could delay valuable domestic cargo shipments. If breached, mine tailings and industrial waste impoundments can harm human health and the environment, as well as affect nearby communities in a manner similar to dam or levee breaching. Such consequences of compromised Dams Sector infrastructure could result in severe economic losses and loss of life.

The following are five major focus areas for Dams Sector security and resilience risk management planning consideration.

Natural Hazards: Adverse events caused by Earth's natural processes, such as floods, tropical cyclones, wildfires, tornadoes, earthquakes, and tsunamis. Natural hazards have the potential to cause substantial loss of life or property damage, as well as economic damage through disruption or destruction of facilities and operations. For the Dams Sector, natural hazards can cause long-term physical damage to sector facilities, disruption of access to facilities, and loss of power and fuel (for back-up power). Dams or levees can fail because of overtopping, piping, or foundation erosion during flooding events. Droughts can interrupt operations because of limited water resources and competing priorities. Other hazards, such as wildfires, can change the hydrology of a watershed and create debris that ultimately affects Dams Sector operations.

Technological Hazards: Issues relating to the age and stability of Dams Sector assets. Such infrastructure and structural issues include erosion and instability related to changing environments or industry practices, lack of maintenance and rehabilitation of decades-old infrastructure, and consequences from population growth and development. The operating environment for the Dams Sector is changing, including different weather and water use patterns, engineering standards, and development around sector infrastructure. Meeting the demand to adapt to such changes can be challenging for owners and operators because of the need to upgrade major infrastructure components, increased safety and security requirements, and funding concerns.

Cybersecurity: Information technology attacks by sophisticated cyber actors and nation-states that exploit vulnerabilities to steal information and disrupt, destroy, or threaten the delivery of essential services. For the Dams Sector, major cybersecurity issues include impacts on operations due to advanced persistent threat attacks, distributed denial of service attacks, malware and ransomware attacks, and malicious manipulation of industrial control systems. Vulnerabilities due to increased connectivity and disruptive digital technology, supply chain threats, and lack of system updates can expand the potential attack surface. The Dams Sector relies on cyber assets to manage, command, direct, or regulate physical processes. Abuse of these controls could cause infrastructure damage, disrupt operations, or cause collateral damage such as upstream or downstream flooding.

Criminal Activities and Terrorism: The unlawful use of violence and intimidation in the pursuit of personal or political aims. Criminal activities and terrorism can take many forms, including chemical, biological, nuclear, radiological, explosive, and mechanical attacks. These attacks can have catastrophic impacts on lives, facilities, and operations. For the Dams Sector, attacks such as those carried out by armed attackers (e.g., active shooter or improvised explosive device incidents), criminal acts, insider threats, suspicious activity, and vehicle and unmanned aircraft attacks have the potential for temporary disruptions in operations or the total loss of a facility. Such disruptions could result in lost power generation, downstream flooding, or reduced availability of water resources.

Crosscutting Issues: Issues stemming from infrastructure, social, technology, and economic changes that have the potential to affect multiple infrastructure sectors, increase capital expenditures, and lead to loss of lives and property. For the Dams Sector, crosscutting security and resilience issues include dependencies and interdependencies with other sectors such as reliance on Communications Sector networks for remote access and control, interconnections with Energy Sector infrastructure to provide or receive electric power, and provision of Transportation Sector services such as navigation locks. Other issues are human factors such as decision-making errors leading to operational failures and the need to rebuild long-term institutional knowledge.

This document provides a sector-specific characterization of relevant factors and decision-making drivers influencing the current operating environment and security and resilience posture of the Dams Sector. Government and industry partners may use this document to help identify and address factors that could have adverse effects on the security or resilience of facilities, personnel, and operations. This document does not represent a compendium of vulnerabilities, nor is it a sector risk assessment. The different factors discussed in this document have been included because they influence the critical infrastructure security and resilience posture of the sector as a whole. Therefore, these factors are discussed from a sector-wide perspective and may not apply to all industry segments within the sector. As the security and resilience operating environment for the Dams Sector changes, this document may be updated.

Natural Hazards

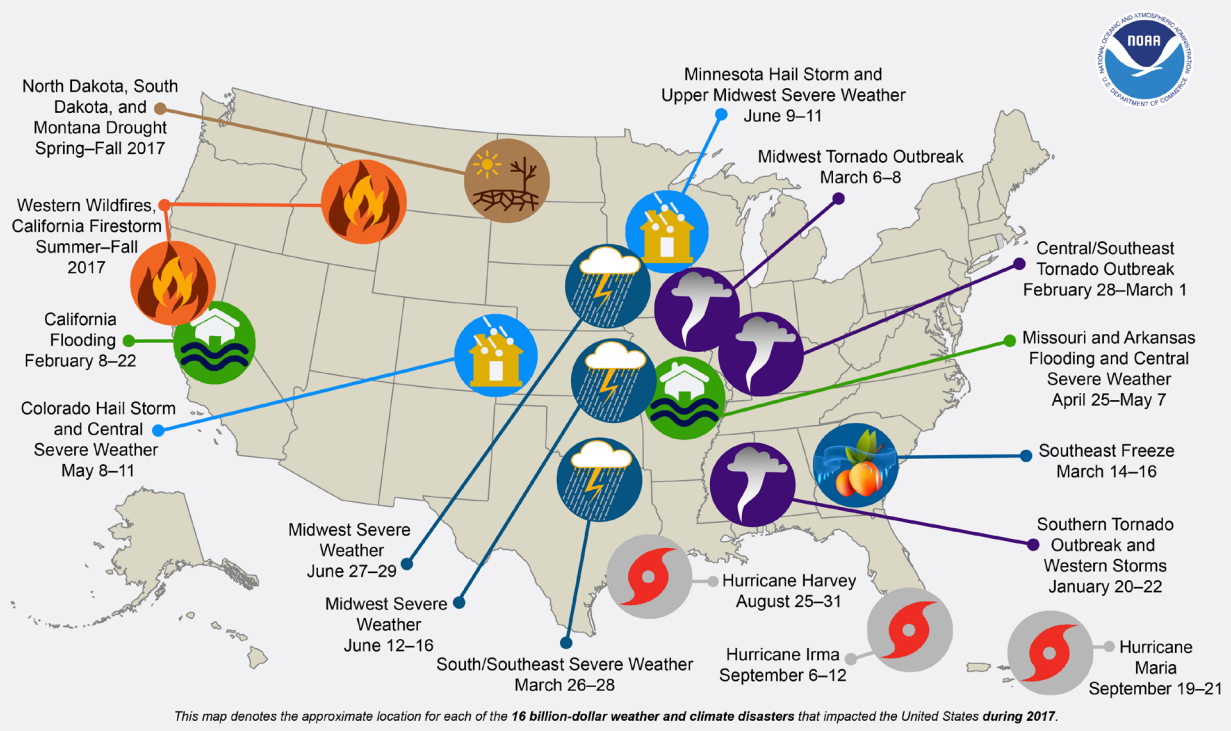
Natural hazards include major adverse events caused by Earth's natural processes, including floods, tropical cyclones, wildfires, tornadoes, earthquakes, and tsunamis. Natural hazards can cause disasters that result in loss of life or property damage as well as economic damage, disrupting or destroying facilities and operations. The severity of a natural disaster is measured in terms of lives lost, economic disruption, and the affected population's ability to rebuild.

Major security and resilience issues for the Dams Sector regarding natural hazards include drought and earthquakes in the Central and Western United States, flooding along the Gulf Coast and in the Central and Western United States, tropical cyclones along the Atlantic Coast and Gulf Coast, and wildfires in the Western United States. Recognizing and addressing these concerns could help to mitigate the financial, operational, and human impacts of natural hazards.

Costly Impacts of Natural Hazards

Recent billion-dollar-loss natural disaster events in the United States included Atlantic and Gulf Coast hurricanes, northeastern winter storms, flooding along the Gulf Coast and in central and western states, freezing in southeastern states, tornadoes and hail storms in central states, and fires and drought in western states. In 2017, the Nation experienced 16 billion-dollar disasters, with total damage costs exceeding $300 billion. The total number of these disasters ties the annual record from 2011, and the total damage cost is a new annual record.[2] Figure 1 provides a map of these events. Such large-scale events have cascading impacts across sectors and regions, with the potential to cause drastic disruptions to Dams Sector facilities and organizations (e.g., long-term physical damage, disruption of access, and power and fuel loss).

Figure 1. *2017 U.S. Billion-Dollar-Loss Natural Disaster Events*
Source: National Oceanic and Atmospheric Administration (NOAA)



- **Long-Term Physical Damage:** Physical damage to Dams Sector facilities from such large natural hazards can be catastrophic, with recovery times extending for months or years. Damage could include dam or levee failures or the destruction of associated facilities such as control centers. Examples of prolonged physical damage and recovery include the New Orleans, Louisiana, area levees damaged by Hurricane Katrina and the damage to Oroville Dam following the 2017 severe flooding in California (see the Oroville Dam Incident Case Study in the Technological Hazards section).
- **Disruption of Access:** Major natural hazards often damage roads or bridges, which can cut off or drastically restrict access to Dams Sector facilities. This hinders response and recovery efforts, limiting the ability of owners, operators, regulators, and other response personnel to assess conditions of the dam and operate the dam's floodgates, if necessary. Lack of access could prevent the closing of floodgates when water storage is needed or the starting of backup generators to power control and security systems. Prolonged limited access can lead to secondary disasters downstream (depending on the facility) as intervention or mitigation activity is delayed.
- **Power and Fuel Loss:** Power outages and disruption of the fuel supply chain (for backup power) are expected during large-scale natural hazard events. Dependence on the Energy Sector to supply power and fuel and respond to their disruption renders the Dams Sector vulnerable to cascading failures (i.e., if a facility is otherwise unimpaired by a natural hazard, it may still be vulnerable to Energy Sector disruptions). The supply chain for large backup generators could include up to a year in lead time and so is of particular concern to Dams Sector owners and operators.

Drought

Many parts of the contiguous United States are experiencing less rainfall than in prior years. Combined with the trend of higher temperatures, reduced precipitation causes drought conditions that deplete reservoirs and create competing needs for a limited, and now diminishing, water supply. Erratic, less-predictable weather patterns complicate the challenge of drought by rendering standard water resource management practices less effective.[3]

- **Weather Variability and Extreme Weather Events:** Droughts in the United States are becoming more frequent and lasting longer. Increased temperatures, persistent droughts, and shifts in weather patterns (e.g., earlier snowmelt and winter rain replacing snow) can greatly affect water resource availability. Continued droughts may deplete water availability while increasing water demand. Conversely, shifting rainfall patterns can create unexpected flooding or increase water availability when it is in less demand. Historical precedents for when rain is and is not expected may be less accurate for water resource management decisions.
- **Shifts in Water Use and Availability:** Lower stream flows caused by drought, upstream dams, and diversions decrease water availability and can reduce the functionality of reservoirs. This is especially challenging for hydropower production and exacerbated by competing demands and operational constraints. For example, shifting precipitation and snowmelt patterns may increase hydropower generating capacity during periods of low demand and/or decrease capacity during peak periods. Flooding can make it difficult for owners and operators to manage hydropower production since water often needs to be released from reservoirs to accommodate flood water.

Earthquakes

Though most Dams Sector structures are relatively resilient to earthquakes compared to other infrastructure and buildings, major earthquakes present a threat to the Dams Sector. A strong earthquake in the San Andreas Fault in California, the Cascadia seismic zone in the Pacific Northwest, or the New Madrid seismic zone in the Central United States could cause significant economic and critical infrastructure damage that

may have impacts on Dams Sector assets (other than the dams or levees themselves) or indirect impacts on Dams Sector operations.

- **Earthquake Resilience:** The historical performance of dams in seismic events has been exceptionally good. Only one concrete dam in modern history has ever failed as the result of a seismic event, mainly owing to the fault running directly beneath it. Generally, concrete dams have sustained only minor damage from earthquakes. The data on the performance of embankment dams is more limited, but the number that have failed as the result of a seismic event is nevertheless extremely small. For example, in the March 2011 9.0 earthquake near Japan, only one small irrigation dam failed (of the 252 dams inspected the day after the earthquake), and six other embankment dams had shallow cracks on their crests but were functioning with no problems. In the February 2010 8.8 earthquake near Chile, no embankment dams failed, and only a few suffered more than minor damage.[4] Mine tailings, however, may be more susceptible to damage from earthquakes. Many mine tailings are built by an upstream construction method that renders them more susceptible to failure if the site experiences a sudden loss of strength (e.g., through liquefaction) during a seismic event.
- **Regional Impacts:** Earthquakes are a significant concern for certain areas of California, the Pacific Northwest, and the Central United States. A major earthquake in the San Andreas Fault,[5] Cascadia seismic zone,[6] or New Madrid seismic zone[7] would severely disrupt critical infrastructure in the affected region. Not only would Dams Sector facilities in the region experience major disruptions directly, the impacts to transportation systems would cripple critical infrastructure supply chains for weeks. Water and power infrastructure could be similarly disrupted. Such an event could lead to several hundred billion dollars in losses for the region and affect many millions of people.

Flooding

Increased likelihood of flooding across many areas of the United States increases risk to Dams Sector facilities. Past major events have threatened Dams Sector operations at locations along the Gulf Coast and major rivers of the Central and Western United States (e.g., Hurricane Harvey, California flooding, and Mississippi River flooding in 2017). The potential for dam and levee failure from overtopping caused by flooding is a significant threat to the Dams Sector. Other failure modes from flooding include internal erosion from seepage —or "piping"—of water passing through an embankment or foundation, or foundation erosion from flood water pressure. The frequency of major flooding events may be increasing across the Nation, making more Dams Sector facilities susceptible to flooding damage than in the past.

- **Overtopping:** Reservoir inflow from storm events that exceeds the available storage and/or spillway discharge capacity can result in a dam overtopping. If overtopping protection fails during a flood event and the underlying embankment is exposed, erosion and headcutting in the embankment materials could progress rapidly. This could lead to a breach of the dam during the flood event, with no potential for preventing the failure. Dam failure from overtopping can lead to a potential for loss of life and significant downstream damages. Overtopping is a common failure mode, accounting for 30 percent of the failures in the United States over the last 75 years.[8]
- **Flash Flooding:** Storms that generate excessive rainfall often cause flash flooding that can quickly overwhelm dams that are not able to withstand such onslaughts of water. Smaller dams may be more susceptible to flash flooding damages. For example, flash flooding caused a dam in rural Wisconsin to fail in June 2018 when the Midwest experienced a series of severe thunderstorms that caused several inches of rain to fall in short amounts of time. The dam failure caused additional flash flooding downstream and damaged roads.[9]

Tropical Cyclones

Tropical cyclones are large, powerful, low-pressure storm systems that typically form over large bodies of warm water. Tropical cyclones include tropical storms, hurricanes, and typhoons. The Atlantic hurricane season has been disastrous for the United States in the recent past. As shown in Figure 1, three hurricanes impacted the United States in 2017, each resulting in more than one billion dollars in losses. Other historical hurricane events such as Katrina, Rita, Ike, Sandy, and Matthew have also shown how catastrophic these events can be to all sectors, and the Dams Sector may be more prone to damages in the regions along the East and Gulf Coasts where tropical cyclones tend to strike.

- **Tropical Cyclone Preparedness:** Dams Sector emergency plans for tropical cyclones involve many actions taken in advance of storms. Depending on the severity of the storm, these actions may include conducting complete shutdown of facilities following strict safety and operating procedures, evacuating personnel, preparing backup power generators, physically securing equipment, and removing unnecessary vehicles and other equipment. Such preparedness actions may affect or halt facility operations and increase expenditures but are important considerations for overall resilience.
- **Tropical Cyclone Impacts:** As major storms such as Maria, Irma, Harvey, Rita, and Katrina have demonstrated, the impact of tropical cyclones can extend well beyond the potential threat to employees and physical damage to facilities and their adjacent communities. Extensive damage to local infrastructure from these events blocked the flow of electricity and natural gas, while damaged roads and rail lines prevented recovery efforts. The Guajataca Dam in Puerto Rico provides a major recent example of Dams Sector impacts from hurricanes. Hurricane Maria caused extensive spillway damage that led to the evacuation of thousands of people in communities downstream.

Wildfires

The area of land burned by wildfires every year in the United States has been trending steadily upward since 1985.[10] The duration of the annual season in which weather conditions are favorable for wildfires has also increased, making wildfires more likely to occur throughout the year. Higher temperatures and drought have made the Western United States prone to larger wildfires, as evidenced by the major wildfires of 2017 and 2018 in the region. Wildfires are often considered natural hazards, yet many are initially caused by humans. Though wildfires are not a major structural threat to dams and levees, the impacts of wildfires can threaten facility functions and operations by limiting access to facilities and changing the hydrology of reservoirs and surrounding watersheds.

- **Access to Facilities:** A wildfire's impacts on access to facilities could be severe. Many dams are remotely located, with surrounding natural areas. An active wildfire could cut off physical access to a facility, as could fallen trees or other debris and damage to roads. Wildfires can similarly interrupt telecommunications access to Dams Sector facilities.
- **Debris and Sediment:** The movement of debris and sediment into waters flowing to a dam during heavy rain can disrupt facility operations and functionality. Wildfires can change the hydrology of a watershed, including how water moves through it and how susceptible the surrounding land is to erosion. Heavy rain on recently burned areas carries downed trees, ash, and other loose debris from fires along flood paths, causing increased runoff and erosion. This runoff and erosion can deposit large amounts of sediment into reservoirs and reduce reservoir capacity. Tree debris and mudslides of fire debris can block access to facilities and obstruct spillways and floodgates.
- **Direct Impact:** Wildfires can damage the surface of a dam or spillway, especially vegetation cover on embankment slopes or in spillway channels. The loss of this vegetation can render the spillway more susceptible to erosion. Wildfires can also damage or impair ancillary facilities set apart from the dam and water (e.g., out buildings or storage facilities), as well as services critical to facility operations,

such as communications and electric power. See the Wildfire Interdependency Incident Case Study in the Crosscutting Issues section for an example of wildfire impact.

Case Study: Flooding in the Carolinas

The October 2015 North American storm complex was an extratropical storm that caused historic flash flooding across the Carolinas. The five-day weather event followed an extended period of rain in late September, so the ground was already saturated when record amounts of rainfall began pelting the region. Over 16 inches of rain fell in the 24 hours of October 4. State-wide impacts to infrastructure included the failure of 49 state-regulated dams, one federally regulated dam, two sections of the levee adjacent to the Columbia Canal, and many unregulated dams. The flooding washed away roads, bridges, vehicles, and homes, and 19 lives were lost. While it is impossible to attribute specific damage to one cause, many faulted dam failures for the extensive losses.

After the storm, the Federal Emergency Management Agency (FEMA) deployed a team to assist with dam assessments, which covered not only the failed structures but also nine that held. Results indicated that most of the failed dams experienced overtopping, with structural failure and piping failure as the second and third most common issues, respectively. Dams that did not fail often had relatively large open channel auxiliary or service spillways that increased the structures' capacity to pass excess flow and volume, potentially preventing overtopping.

None of the high-hazard-potential dams received rainfall amounts greater than the maximums specified in regulations, but most of the dams experienced upstream breaches that likely contributed to the failures. All dams were constructed prior to the enactment of the South Carolina Dams and Reservoirs Safety Act, although several had undergone post-Act modifications.

The final FEMA assessment report of the dam failures included extensive recommendations to the South Carolina Department of Health and Environmental Control, from planning approaches (e.g., developing hazard mitigation plans) to structural approaches (e.g., increasing spillway capacity) to decommissioning dams (e.g., dams with damage so extensive that repair costs outweigh benefits). The report also provided recommendations for improving collaboration between internal and external FEMA partners.

Technological Hazards

The average age of the Nation's dams and levees is over 50 years. When dams are properly maintained and rehabilitated to meet current standards, aging is not a major concern. Many aging U.S. dams, however, require significant modifications or rehabilitation to meet current conditions and to continue to operate at a high level of safety and security.

Major security and resilience issues for the Dams Sector regarding technological hazards include safety issues from risk of failure and increasing hazards and deficiency, erosion and instability related to changing environments or industry practices, maintenance and rehabilitation of decades-old infrastructure, and threats from population growth and development.

Dam Safety

Safe operation and maintenance are at the forefront of Dams Sector security and resilience. Approximately 70 percent of dams in the United States are state-regulated. The Federal Emergency Management Agency (FEMA) Model State Dam Safety Program was developed to assist state officials in initiating or improving their state dam safety programs. The program outlines and provides guidance on the key components of an effective dam safety program to reduce the risks created by unsafe dams. Since the establishment of the program, average state dam safety program performance has consistently improved across those key components.[11] However, dam failures can and have occurred in the United States, causing loss of life and severe economic and environmental damage. Major issues relating to dam safety for owners and operators include the risk of dam failure, increasing hazards, and increasing deficiencies of aging dams.

- **Risk of Failure:** The risk of dam failure is the overall driving force for all dam safety activities. Though the majority of dams in the Nation are safely operated and properly maintained, failures can still occur. According to the Association of State Dam Safety Officials (ASDSO), states reported 173 dam failures from 2005 to 2013.[12] As dams across the Nation increase in age, the risk for failure also increases. Major failure modes of concern for owners and operators are described in the Erosion and Instability section, below.
- **Increasing Hazard:** Dams are inherently hazardous structures owing to the potential for significant economic and environmental damage, or even loss of life, from a complete or partial dam failure. Dams are classified by states and the United States Army Corps of Engineers (USACE) as high hazard potential if their failure could cause loss of life. This classification refers to the consequences of failure, not the condition of the dam. Approximately 15,000 of the 90,000 dams in the USACE National Inventory of Dams (NID) are classified as high hazard potential.[13] This figure increases as economic development occurs downstream of dams, influencing the safety requirements and activities for owners and operators (see the Population and Development section, below, for more information).
- **Increasing Deficiency:** States and USACE identify deficient dams as those that have hydraulic or structural characteristics that render the dams more susceptible to failure. The number of high hazard potential dams identified in the NID as deficient and in need of repair has steadily increased in the past 15 years.[14] Significant investment in the rehabilitation of these dams will be required to maintain a high level of safety in the Dams Sector (see the Maintenance and Rehabilitation section, below, for more information).

Erosion and Instability

The vast majority of dam and levee structure failures worldwide are due to internal and external erosion, while a lower percentage are due to instability. In addition to erosion as a major failure mode, foundation defects, including settlement and slope instability, account for a significant portion of U.S. dam and levee failures. The changing operating environment for Dams Sector facilities and the evolution of engineering practices and standards (industry and regulatory) for dams and levees may be influential factors in dam and levee erosion and instability.

- **Operating Environment Issues:** Conditions surrounding the operation of dams have changed since many of the dams were built. Changing weather patterns such as the increased frequency of extreme flooding events, earlier springs and snowmelt, and increased likelihood for wildfires have added to the potential for erosion of embankments, spillways, and reservoir boundaries. Many dams and levees were not designed and built to address such conditions.
- **Engineering Advancement and Standards:** Understanding of engineering and construction has evolved over time since many dams and levees were built (e.g., from stone masonry in the 1800s, to reinforced concrete in the early 1900s, to advanced roller compacted concrete in the 1980s and into the 21st century). Industry and regulatory standards for dam and levee engineering and construction have changed in response. Standard and acceptable practice in these fields 50 years ago or more may be out of date, and older dams may be more vulnerable to certain types of erosion or instability. Many earthen dams built prior to 1970 were founded on granular alluvial deposits. Many of these alluvial deposits are susceptible to erosion through liquefaction, especially in areas of higher seismic activity.
- **Construction Issues:** Construction flaws, including the use of sub-optimal materials and errors in decision-making (see Workforce Issues in the Crosscutting Issues section), can exacerbate erosion and lead to instability of dams and levees. For example, an earthen dam in North Carolina was breached by a major flood in 2003. The dam was rebuilt with concrete in 2008, yet it failed two years later from erosion, in part because of deviations in construction from the design plans.

Maintenance and Rehabilitation

Many Dams Sector assets were built decades ago and require routine maintenance to operate safely and securely. Some may require rehabilitation to meet improved safety criteria or address newer or emerging threats. Large-scale repair and rehabilitation are challenging for Dams Sector owners and operations because funding for such long-term expenditures is limited.

- **Life-Cycle Upgrades:** Many Dams Sector components were built for long-term durability, intended to last for many decades. Major upgrades are often required at the end of the life cycle of critical components (e.g., turbines and transformers). Often these critical components were designed for the specific site where they operate and are unique, making replacement and upgrading a costly and time-consuming process.
- **Funding Concerns:** Maintenance and rehabilitation of Dams Sector infrastructure involve significant capital expenditures. ASDSO estimates that rehabilitation of federal and non-federal U.S. dams could cost more than $70 billion.[15] Dams Sector owners and operators conducting business on existing tight budgets are concerned with funding the necessary improvements to sector infrastructure for ongoing safety and security. The capacity of Dams Sector owners and operators to maintain and repair their facilities varies widely, as owners and operators range from large electric power utilities to states, counties, cities, and small private businesses. Many owners and operators do not have personnel expertise to apply for government grants or develop technical architectural and engineering contracts to support maintenance and rehabilitation. Such gaps in capabilities can lead to delays and deferred maintenance, improvements, and repairs.

Population Growth and Development

Growth in population and industrial development around dams and levees increases the potential consequences for downstream communities in the event of dam or levee failure. Farmland and undeveloped areas located around dams are increasingly replaced by developed communities. As population growth around dams and levees increases, new operating concerns arise for assets that were designed without the implications of risk to downstream communities. Consequently, the number of dams classified as high hazard potential is increasing with population growth and development.

- **High Hazard Potential:** U.S. dams were engineered and constructed relative to the hazards of the time. Dams that had the potential to cause loss of life in the event of failure were designed and built with stricter safeguards than those that would have less drastic impacts upon failure. As development encroaches on areas downstream of dams, the potential for disasters rises, and dams that were once in unpopulated areas subsequently elevate to a higher level of risk. As a result of increased development, the number of dams classified as high hazard potential by USACE increased by 50 percent from 2005 to 2015.[16]
- **Adapting to Development:** Increased development around dams and levees can increase the demands placed on the infrastructure and the water resources it provides. Higher populations and industrial complexes added to the areas require more water to operate and thrive. Increased water use can decrease reservoir levels, which can have an impact on the effectiveness of dam operations (e.g., lower water levels affecting hydropower). Similarly, increased populations have higher demands for power, which could stress hydropower facilities. Owners and operators may be challenged by the need to adapt to such new demands, including incorporating updated requirements for safety and security to coincide with increased hazard potential (e.g., raising the dam crest height or increasing the capacity of the spillway system to accommodate larger storms or flood events).

Case Study: Oroville Dam Incident

The 2017 California floods took a toll on much of the state's infrastructure, including Oroville Dam. In February of that year, the main and emergency spillways of the dam were damaged, leading to the evacuation of more than 180,000 people living downstream along the Feather River.

The excessive water continued through cracks and joints in the spillway chute slab, resulting in uplift. The uplifted slab section, in turn, exposed the foundation rock, which was of poor quality, to the floodwaters. The rock quickly eroded, causing removal of additional slab sections, which led to more erosion.

Decision makers closed the spillway gates and, over the following few days, tried to determine a path forward. Reopening the gates would cause further damage to the main spillway; leaving them closed would allow lake levels to rise and overtop the emergency spillway weir. The final strategy sought a balance, with occasional releases through the service spillway, but the decision makers erred on the side of too few discharges, causing overflow of the emergency spillway.

The incident had no single cause but rather resulted from a long-term systemic failure across many players and factors, beginning with dam construction and continuing through the event. For example, the dam's construction was not well modified to fit the site conditions, regular inspections did not uncover the structure's inherent weaknesses and deterioration, and final decisions went against the advice of civil engineering and geological personnel.

Lessons learned for dam owners include going beyond minimal compliance with regulatory requirements; developing and maintaining mature dam safety management programs; supplementing physical inspections with comprehensive reviews of original design, construction, and subsequent performance; giving attention to appurtenant structures such as spillways; and conducting critical reviews of Potential Failure Mode Analysis (PFMA) processes.

Cybersecurity

The Dams Sector is subject to a wide range of risks stemming from cyber threats and hazards. Sophisticated cyber threat actors and nation-state actors exploit vulnerabilities to steal information and disrupt, destroy, or threaten the delivery of essential services. As information technology (IT) becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide-scale or high-consequence events.

Issues of higher cybersecurity risk for the Dams Sector include advanced persistent threat (APT) attacks, distributed denial of service (DDoS) attacks, threats to industrial control systems (ICSs), increased connectivity and disruptive digital technology, vulnerabilities from the Internet of Things (IoT), malware and ransomware, supply chain threats, and insecurity due to lack of system updates. Recognizing and mitigating these issues could help to limit cyber intrusions.

Advanced Persistent Threat

Coordinated long-term cyber campaigns by motivated groups pose significant risk to the Dams Sector. Opportunities for long-term cyberattacks will likely always exist in both cyber assets and the personnel who use them, and APTs can exploit these opportunities given enough time and resources. APTs may be able to establish a foothold in a facility's network and move laterally or probe deeper into internal networks undetected to attack ICSs. Developing attacks on ICSs takes time, knowledge, and expertise in the unique operating environments of the target facility. APTs therefore take advantage of vulnerabilities at multiple stages to gather information and develop and validate their attacks. VPNFilter, Dragonfly, and Hatman are three recent notable examples of malware that, because of their sophistication, appear to have originated with an APT group; and all three targeted, or had the ability to target, critical infrastructure.

- **VPNFilter:** In May 2018, Cicso's Talos Intelligence Group announced its research into a modular malware system named VPNFilter, which had infected more than 500,000 devices. The malware uses vulnerabilities in a range of network devices—primarily internet routers—to install a persistent foothold in the targeted devices, which can be used to deploy further modular malware on the device. Parts of the code used in this platform overlap with the BlackEnergy malware used to target Ukrainian electric utilities, and modules exist that extend the malware's capabilities to monitor for Modbus network traffic, a common protocol used in ICSs.[17]
- **Dragonfly:** Russian government cyber threat actors have been targeting U.S. critical infrastructure sectors since at least March 2016 in a coordinated campaign of malware attacks collectively named Dragonfly. The threat actors used a combination of spear-phishing (highly targeted emails with malicious attachments) and watering hole attacks (introducing malware through well-known industry trade publications' websites) to collect user credentials. The threat actors were able to establish footholds in the target networks and conduct network reconnaissance, move laterally, and collect information pertaining to ICSs.
- **Hatman (also known as TRITON and TRISIS):** This attack platform targets safety controllers manufactured by a major international ICS provider. Safety controllers play an essential role in ICS environments to ensure the safe and predictable shutdown of operational equipment. Hatman malware was specifically designed to allow changes to the safety controller to introduce new functionality that would likely degrade the safety controller's ability to shut down unsafe equipment safely.

These types of intrusions can lead to malicious actors taking full control of network infrastructure, allowing for further attacks on connected infrastructure (e.g., data theft, espionage, denial of service, or decreased functionality).

Distributed Denial of Service Attacks

DDoS attacks are a growing threat, using many Internet-connected devices to generate immense bandwidth loads to the point of disruption or creating openings for malware to be deployed. As the Dams Sector introduces more Internet-connected devices into its processes (see Internet of Things below), threats from DDoS attacks also increase. Common security devices that use high-bandwidth connections, such as security cameras and digital video recorders in Dams Sector facilities, are of particular concern for DDoS attacks because they can suddenly consume large volumes of Internet traffic and are commonly deployed in large batches.

- **Botnets:** Botnets are a collection of Internet-connected devices that have been infected with malware to respond to specific requests from a command and control entity. Potential devices range from home computers to IoT devices. Botnets can be used to generate massive amounts of Internet traffic to a specific target with the intention of disrupting essential services. A recent high-profile example was the Mirai botnet, which was used in October 2016 in a DDoS attack on a major domain name system (DNS) service provider. The attack flooded 1.2 Tbps of Internet traffic (at the time, the highest volume of DDoS traffic ever recorded) managed by the DNS provider and shut down many well-known websites. At the height of the attack, millions of users were denied Internet services in North America and Europe. Similar to a previous September 2016 Mirai attack, the DNS attack also employed millions of compromised Internet-connected security cameras to simultaneously conduct the attack.[18]
- **Amplification:** In amplification, a cyber threat actor abuses Internet-connected devices so that they respond to a small packet of code from the attacker by sending large packets of data to a target as part of a DDoS attack. The effect amplifies the bandwidth sent by the threat actor, resulting in much larger amounts of data flooding the target. Unlike with botnets, the attacker does not necessarily need control of the device. Instead, a threat actor abuses the devices' intended functionality to respond to requests and causes the responses to flood a target's servers. Memcached DDoS attacks, a specific type of amplification attack, resulted in 1.3 Tbps and 1.7 Tbps of Internet traffic in separate attacks in March 2018, though no critical services were disrupted.[19]

Increased Connectivity and Disruptive Digital Technology

Combining physical and digital technologies in the Dams Sector can lead to increased points of access through which malicious code could be introduced or data could be stolen, as well as cascading failures between devices due to interconnectivity.

- **Increased Points of Access:** An expanding footprint of networked devices introduces more points of potential targets for cyberattack in a network. This includes both physical (e.g., locations for input or display devices) and cyber (e.g., network ports) points of access that could be exploited.
- **Cloud Services:** Dams Sector organizations are increasingly incorporating cloud services into their business operations. Cloud software-as-a-service (SaaS) is leveraged to enhance business functions in the areas of IT, human resources, marketing, and supply chain. Although cloud services offer benefits, such as scalability, high availability, advanced data analysis and storage, and decreased ownership cost, new cybersecurity concerns are associated with those benefits. Cloud services share many of the same cybersecurity issues as physical IT (e.g., denial of service, APT, stolen credentials, and phishing), yet also exhibit virtual susceptibility to attacks, including malicious control of virtual machines and attacks on systems running virtual processes.
- **Cascading Failures:** Automated systems that are dependent on interconnected devices may be subject to cascading failures that result from disruptions along the network of devices. Similarly, process flow disruption or alteration (whether intentional or accidental) within a chain of interconnected devices can have drastic cascading effects on facility operations and safety. For

example, networked building automation control systems such as access control, fire suppression, and heating, ventilation, and air conditioning (HVAC) can influence each other. A failure of an HVAC component could delay the activation of fire suppression in the event of a small fire, causing more damage as the fire spreads.

Industrial Control Systems

ICSs are vital to the efficient and safe operation of many Dams Sector facilities because these systems typically manage, command, direct, or regulate physical processes at the facility. Control systems can have decades-long life cycles and typically place priority on uptime and reliability. Older ICSs were often isolated from wider networks and relied on proprietary software that created a knowledge barrier for cyber threat actors. As the Dams Sector advances in technical complexity, increased ICS automation and connectivity that can improve operability and efficiency also introduce new cybersecurity issues. Newer ICSs are highly networked and use common and open standards for communication protocols as well as common operating systems, creating potential to expose assets to cyberattacks.

Unauthorized Dams Sector control systems access could allow cyber threat actors to remotely direct physical processes and cause infrastructure damage, disrupt operations, or cause collateral damage (e.g., upstream or downstream flooding, disruption of water supply, power disruptions, or impacts on transportation systems). Cyberattacks on ICSs are advancing in complexity, sophistication, and volume, leading to new methods of infiltration and disruption. The number of known cyber vulnerabilities of ICSs across all sectors has steadily increased since 2010.[20] Common high-risk cyber issues related to ICSs include increased connectivity and complexity of ICS assets, long-term legacy of many ICSs, Internet exposure through cloud services and remote access, and foreign ICS suppliers and contractors.

- **Connectivity:** ICSs that rely on highly specialized, vendor-specific operating platforms are increasingly connected to facility business systems that rely on common operating platforms, which are accessible through the Internet. This connectivity introduces potential attack vectors that have not been a concern for ICSs in the past (e.g., phishing, malware, and ransomware attacks that originate through email or Internet browsing). In addition, ICS components or business system components connected to ICSs that use wireless communication are susceptible to infiltration and attack from outside the ICS or business network.
- **Complexity:** The demand for real-time monitoring or control has increased system complexity. For example, ICS access is being granted to more users, business systems and ICSs are increasingly interconnected, and the degree of interdependency among critical infrastructures has increased. In addition, differences in the training and focus of those managing IT systems and those responsible for control system operations have also led to challenges in coordinating network security between these two key groups (e.g., different priorities, methodologies, and expertise).
- **Legacy Systems:** Some older ICSs were designed to operate in more independent modes than modern systems but have subsequently been integrated into networked controls. Older systems tend to have inadequate account and security administration. Some systems may have hard-coded or default credentials such as static passwords and access keys that allow an attacker to easily pass authentication requirements, gaining malicious control of networked ICS devices, which could allow for remotely conducted attacks.
- **Cloud Services:** In addition to being leveraged for business applications, the use of cloud computing with industrial control processes is becoming more common. Some Dams Sector organizations use cloud services to store, manage, and process control systems data rather than using local servers or computers. This introduces additional cybersecurity concerns traditionally not related to ICS (see previous item on cloud services).
- **Remote Access:** Dams Sector organizations increasingly control ICSs through remote means, such as virtual private networks (VPNs), to grant employees secure remote access to their computing and

control resources. However, cyber threat actors continually look for weaknesses in VPN implementation and develop methods to circumvent VPN security and gain remote access to control systems and networks. Even limited connection to the Internet of ICS components exposes ICSs to malicious cyberattacks.

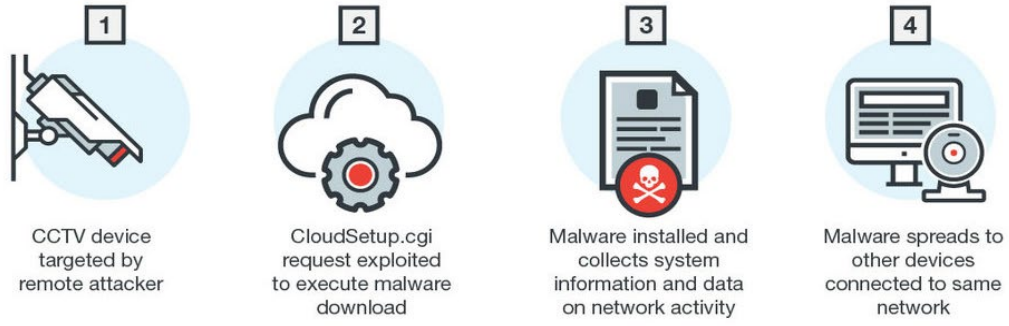
- **Offshore Reliance:** ICSs often have no feasible alternatives to the use of commercial, off-the-shelf products. Many software, hardware, and control system manufacturers are under foreign ownership or develop systems in countries whose interests do not always align with those of the United States. The practice of contracting ICS support, service, and maintenance to third parties located in foreign countries also introduces risk.

Internet of Things

Internet-connected devices, commonly referred to as IoT, are becoming more commonly used in the Dams Sector for monitoring and optimizing facility processes, sharing real-time data among devices, and sending alerts for faults or deficiencies. The rising use of IoT in the sector, as well as all over the world, leads to increasing cybersecurity issues, such as more opportunities for sector devices to be attacked, increased likelihood that unrelated consumer-level devices will be used against sector infrastructure, and business operations' susceptibility to DDoS attacks.

- **Multitude of Devices:** Increasing the number of IoT devices in use by Dams Sector operations increases the number of ways sector organizations can be attacked. Wireless communication between IoT devices in sector facilities often transmits proprietary or confidential information on processes or business operations. This information could be stolen in reconnaissance operations, or this connectivity could be abused to move within a network or to spread malware—whether remotely, internally through an insider, or in proximity to the facility. Figure 2 provides an example of IoT malware delivery.
- **Dams Sector Operations as a Target:** Cyber threat actors seeking to harm or exploit Dams Sector organizations may employ many external IoT devices (e.g., consumer-level appliances or network devices) in coordinated attacks for control systems surveillance, disruption of operations, or destruction of property.
- **DDoS Attacks:** As described in the above section on DDoS, IoT devices can be exploited to carry out distributed attacks. The malware triggers vast consumption of network bandwidth and can compromise the performance of the infected devices and network.

Figure 2. *Example Infection Pathway of IoT Malware*
Source: Trend Micro



Malware and Ransomware

Malware and ransomware are common attacks on all business IT networks and can infect Dams Sector organizations as well. Malware (a term derived from "malicious software") is the mechanism by which

cyberattacks are carried out. The variety of malware affecting IT continuously expands. In 2017, nearly 670 million new variations of malware were discovered by a major cybersecurity provider.[21] Ransomware attacks are on the rise across all sectors, and business systems are at increased risk of attack. Ransomware is a type of malware that cyber threat actors use to deny access to systems or data by encrypting the files and data on the infected computer. Typically, the threat actor requests a ransom in exchange for decrypting the data and returning functionality. During 2017, the monthly rate of ransomware attacks on businesses in the United States increased tenfold, and the number of ransomware detections by a major cybersecurity vendor increased by 90 percent.[22] Also in 2017, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center received 1,783 complaints identified as ransomware with adjusted losses of over $2.3 million.[23] Examples of large-scale ransomware attacks include the May 2017 "WannaCry" attack and the April 2016 attack of a U.S. utility company.

- **Phishing:** One of the most common mechanisms by which malware is delivered to IT systems and networks is phishing, which is a type of social engineering (i.e., manipulating interpersonal relationships). Phishing refers to malicious emails designed to trick the recipient into opening a malicious attachment, visiting a malicious website, or sharing sensitive information (e.g., passwords, account numbers, or personal information). Spear-phishing is a more targeted form of phishing intended to inflict malware on or solicit confidential or sensitive information from a specific person or organization. The number of phishing emails and compromised vendor email accounts targeting multiple utility industries has increased in the recent past. In 2017, spear-phishing was the most often employed attack vector in targeted cyberattacks.[24]
- **WannaCry:** Organizations all over the world discovered their systems were encrypted by the WannaCry ransomware in May 2017. WannaCry exploited security vulnerabilities released in leaked National Security Agency documents and spread by infecting Windows computer systems not patched to eliminate the security vulnerability. Although the ransomware affected mostly business control systems, the malware mechanism used could be adapted to disrupt process control systems or ICSs (which could have catastrophic effects for critical infrastructure).
- **Business Network Threat to Control Systems:** Malware and ransomware attacks commonly target business networks, but for industries that rely on ICSs, such as in the Dams Sector, control systems may be threatened as well. A municipal water and power company announced its corporate network had been compromised by ransomware in April 2016. The attack was carried out through an infected email attachment opened by an employee. In response, the company disclosed the attack (the first of its kind reported in the United States), shut down its corporate network, ensured that plant operations and ICSs were not compromised, and worked on developing a solution. Ultimately, the company paid the ransom to decrypt its email and accounting systems.

Supply Chain Cybersecurity

Dams Sector assets and networks are susceptible to compromised vendor communications associated with the supply chain. Email phishing attempts from presumed trusted vendor email accounts are becoming more frequent. Successful phishing attempts could allow attackers remote access to enterprise networks and the opportunity to escalate attacks to operations infrastructure. Trusted contractors and vendors may have legitimate remote access to provide services; however, this access could turn problematic if the contractor or vendor has been compromised. The supply chain for software itself represents another cybersecurity concern, as compromised software introduced along the supply chain could be used to attack Dams Sector networks. In addition, cyber threats to the supply chain are interconnected with physical security.

- **Third-Party Attacks:** Cyber threat actors have targeted critical infrastructure subcontractors' networks to abuse access the subcontractor might have to the target organization. This abuse of trust in software suppliers and subcontractors can affect even well-protected organizations.

- **Software Supply Chain:** In 2017, software supply chain attacks increased dramatically across all sectors.[25] By attacking software providers, cyber threat actors replace legitimate business software with maliciously modified versions, unbeknownst to end users. For example, Dams Sector entities may try to install the latest version of previously trusted software, unwittingly downloading a malicious version instead.
- **Cyber and Physical Security Convergence:** Supply chain impacts to cybersecurity can also affect physical security. The converse is also true: physical security supply chain impacts can affect cybersecurity. For example, compromised software used in an ICS could cause ICS network instability and lead to failure of physical operations of the ICS. Counterfeit hardware introduced into physical control systems—such as electronic door locks or security cameras—could render a facility vulnerable to specific cyberattacks.

System Updates

Corporate IT systems that have not been updated with current security patches (for operating systems or software) are a significant cybersecurity issue for the Dams Sector. Some software providers might not provide software patches because the providers lack the ability to distribute patches or the software is beyond the support life cycle and no longer supported. Facility owners and operators might not implement available patches to update devices because the updates would interrupt operations or have unexpected consequences in critical assets. Processing, tracking, and managing patches for alerts from multiple software vendors can be challenging, especially when coordinating internal responses to maintain IT systems' security. Regardless of the reason, unpatched assets remain exposed to known vulnerabilities, which APT actors can exploit or other cyber threat actors can use opportunistically. For example, the WannaCry ransomware, discussed above, propagated quickly and widely in part because many machines remained unpatched and susceptible to an exploit, despite the availability of a security patch.

- **Cost of Breaches:** According to an international study of a major IT and cybersecurity company, cyberattacks in 2017 cost business victims anywhere from less than $100,000 to more than $1,000,000.[26] In 2017, there was a 13% increase in overall reported vulnerabilities and a 29% increase in ICS vulnerabilities. Even though only 6% of breaches in 2017 were attributed to vulnerabilities that could have been patched, keeping systems up to date is widely considered a best practice. In particular, patching systems reduces the risk from opportunistic threats that scan the whole Internet for any vulnerable device. IoT and mobile devices both represent new asset types with vulnerabilities to remediate with updates, which highlights the importance of asset and patch management.[27]
- **Preventable Widespread Attacks:** The WannaCry ransomware spread quickly and widely—infecting computers in more than 150 countries including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan—because it exploited a vulnerability in a common network file-sharing protocol (present in older versions of Microsoft Windows) to propagate itself from one victim to the next. A patch for the vulnerability was released in March 2017, an exploit for this vulnerability was leaked in April, and the outbreak of WannaCry ransomware occurred in May. Despite the availability of a patch two months before WannaCry infected machines worldwide, many machines remained unpatched until after the ransomware was actively spreading to thousands of victims.[28]

Case Study: Industrial Control System Cyberattack

In 2013, seven Iranian cyber threat actors attempted to infiltrate the Bowman Avenue Dam, a small structure in Rye Brook, New York, about 25 miles north of New York City. The hacking strategy involved ongoing DDoS attacks, which ultimately allowed the threat actors access to the dam's control system, seemingly through a cellular modem. The successful breach could have allowed the threat actors to release water from behind the dam. However, at the time of the attack, the sluice gate had been manually disconnected for routine maintenance, and the attack was ultimately ineffective.

The event was part of a series of coordinated cyberattacks largely directed toward U.S. financial institutions, in which banks lost millions of dollars in remediation costs. While not seen as particularly sophisticated, the attacks drew attention to the relative vulnerability of U.S. critical infrastructure to cyberattack—and the interest abroad in exploiting such targets.

Criminal Activities and Terrorism

Criminal activities and terrorism affecting critical infrastructure make headlines around the world almost every day. Terrorism, which can be described as the unlawful use of violence and intimidation in the pursuit of ideological aims, can take many forms, including chemical, biological, nuclear, radiological, and explosive attacks.

In the Dams Sector, security and resilience issues regarding criminal activities and terrorism include armed attacks, criminal acts at dam facilities, the threat of malicious insiders, suspicious and unexplained activities at facilities, and attacks by use of vehicles and unmanned aircraft systems (UASs). Recognizing and mitigating these issues could help to limit the financial, operational, and human impacts of criminal activities and terrorism.

Armed Attacks

Deliberate attacks on Dams Sector assets and personnel by armed assailants could include active shooter incidents (attacks with firearms) or attacks with improvised explosive devices (IEDs). Injury and loss of life are the obvious impacts of such attacks. An IED attack could destroy critical facility assets and threaten the safe operation of the facility, putting nearby and downstream communities in danger. Dams Sector facility operations can also be affected through the loss of employee hours and downtime from compromised equipment or facilities caused by armed attacks.

- **Active Shooter Incidents:** The frequency of active shooter incidents in workplace environments across many sectors has increased in recent years. From 2000–2017, 250 active shooter incidents occurred in the United States, with the average annual number of incidents increasing from 7 (2000–2008) to 20 (2009–2017).[29]
- **Incident Timing:** Armed attacks are dynamic and quickly evolve. Often, the immediate deployment of law enforcement is required to stop the aggressive action of an attacker to mitigate harm to potential victims. However, because such situations are also frequently over prior to the arrival of law enforcement, Dams Sector organizations must be prepared both mentally and physically to address an active shooter situation prior to law enforcement arrival.
- **Operational Impacts:** Facilities and equipment may be damaged from firearms or explosions and removed from service for repairs. Operations may be halted because of the need to investigate a crime scene, which could last for weeks. Employees may not be able to return to work for an extended time because of injuries, psychological impacts, and/or the closure of a facility.

Criminal Acts

Crimes against Dams Sector assets not tied to terrorism can include other threats, such as property crimes, which are a significant concern for Dams Sector organizations. The sector is particularly susceptible to vandalism, arson, burglary, and theft (especially of copper). These crimes can lead to temporary disruptions in operations or the total loss of a facility.

- **Vandalism:** Vandalism is the willful or malicious destruction or defacement of public or private property. Typically, vandalism involves relatively minor destructive crimes (e.g., damaging perimeter barriers, breaking windows, tampering with security cameras, or external defacing of buildings, walls, or dams themselves). However, vandalism could be severe enough to cause major destruction of facility property. The act could also be an indicator of intent for more serious malicious activity against Dams Sector facilities and nearby or downstream communities.

- **Arson:** Arson is the malicious burning of personal or real property with fraudulent or criminal intent. Arson can be considered a more serious form of vandalism in which major assets could be severely damaged or completely destroyed by fire. Arson at a Dams Sector facility could halt operations, cause explosions, and threaten the safety of personnel and nearby or downstream communities.
- **Burglary:** Burglary can be generally defined as the unlawful entry (whether breaking and entering or merely walking through an entry) into a building or structure with the intent to commit a crime. The intended crime in a Dams Sector facility may be theft of valuable material (see the next item), damage to control or security systems, or surveillance toward more malicious activity.
- **Copper Theft:** Copper theft is a major criminal activity issue for the Dams Sector. The price of copper by weight has been at historical record highs since 2005, and theft of copper in the form of electrical wires and scrap metal has increased nationwide over the same time period.[30] Industries that typically use large quantities of copper (including communications, energy, dams, and IT) are increasingly susceptible to copper theft. The damage caused by such thefts is commonly multiple times the value of the copper stolen, requiring major repair costs.[31] Criminals may target Dams Sector hydropower facilities for theft of copper used in power generation and transmission facilities.
- **Other Theft:** Theft issues for the Dams Sector not associated with copper include that of sensitive business or customer data, access controls (e.g., identification and/or key cards), and sensitive, specialized equipment.

Insider Threats

The insider threat can be described as an insider using his or her authorized access, wittingly or unwittingly, to do harm to the organization's resources, personnel, facilities, information, equipment, networks, or systems. Insiders may be employees, former employees, business partners, contractors, consultants, temporary personnel, interns, or vendors. Dams Sector organizations should be familiar with the following practices: identifying behavioral indicators of potential insider malicious acts; implementing insider threat mitigation best practices; vetting personnel thoroughly before hiring; and recognizing, monitoring, and reporting on suspicious activities.

- **Behavioral Indicators:** Behavior traits that may indicate an employee may act or is acting against the employer include disgruntlement; dissatisfaction; and persistent anger, anxiety, or negative attitude. Although insiders intent on doing harm to others or themselves in the workplace may show some visible signs of discomfort or being disgruntled, they may also take steps to avoid drawing any attention to themselves, knowing that behavioral indicators may lead to detection.
- **Suspicious Activities:** Suspicious activities unrelated to an individual's job duties that may indicate an insider threat include collecting excessive information or data (especially of a sensitive nature), frequent unexplained travel, or working uncommon hours without approval.
- **Mitigation Actions:** Best practices for insider threat mitigation include determining behaviors and suspicious activities to monitor, developing clear reporting and investigating mechanisms, and training employees on recognition and reporting. Detecting and mitigating insider threats will almost always rely on the identification of concerning workplace behaviors in combination with select types of suspicious activity. Organizations should develop clear standard mechanisms for reporting and investigating possible insider threats, including provisions for confidential reporting to protect legitimate whistleblowers. In addition, well-informed and -trained employees are the most effective resource to prevent, identify, deter, and respond to insider threats.
- **Personnel Vetting:** Thoroughly examining and identifying the potential for malicious insider activity is imperative to reducing vulnerability to insider threat. This examination should start during an organization's hiring process and continue after the hiring process concludes. Important considerations for vetting potential personnel (employees as well as contractors and subcontractors)

include procedures to properly evaluate personnel and contractor information (e.g., background checks), compliance assessments of personnel regarding insider threat policies and procedures, and a process to facilitate sharing information from human resources, law enforcement, and other pertinent sources to recognize the presence of an insider threat.

Suspicious Activity

Suspicious activities are irregular or highly unusual behaviors that may be associated with pre-operational or preparatory surveillance, operational activities exploring or targeting a Dams Sector facility or system, or any possible violation of law or regulation that could compromise a sector facility or system, jeopardizing life or property. Several types of suspicious activities may occur at Dams Sector facilities, as shown in Table 1. Recent suspicious activities at Dams Sector facilities include attempted intrusions, theft, expressed or implied threats to facilities, information gathering, and photography. Securing Dams Sector facilities (especially those with an extended spatial footprint that includes recreational areas) requires situational awareness regarding such suspicious activities.

Table 1. *Suspicious Activity Types*

Suspicious Activity Type	Description
Attempted Intrusion	Unauthorized personnel attempting to enter, or actually entering, a restricted area or protected site; impersonation of authorized personnel (e.g., police, security, or janitorial staff)
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification to misrepresent one's affiliation to cover possible illicit activity
Theft/Loss/Diversion	Stealing or diverting something associated with a facility (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents)
Sabotage/Tampering/Vandalism	Damaging, manipulating, or defacing part of a facility or protected site
Cyberattack	Compromising, or attempting to compromise or disrupt, an organization's IT infrastructure
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility or infrastructure
Aviation Activity	Operating an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people or property, which may or may not be a violation of Federal Aviation Regulations
Eliciting Information	Questioning individuals at a level beyond mere curiosity (a degree of interest that would arouse suspicion in a reasonable person) about particular facets of a facility's or building's purpose, operations, or security procedures
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person

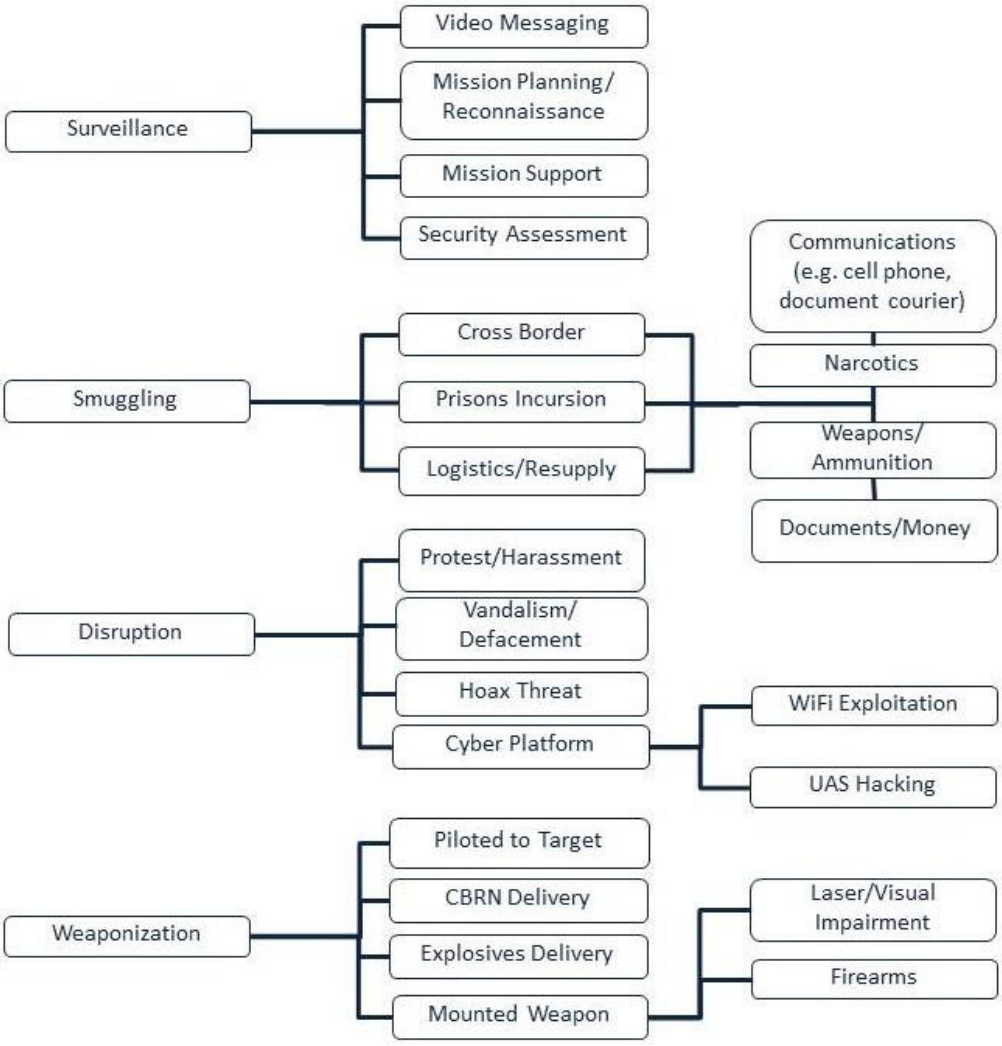
Suspicious Activity Type	Description
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineering) interest such that a reasonable person would consider the activity suspicious
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts, military weapons or tactics, or other unusual capabilities that would arouse suspicion in a reasonable person
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person

Unmanned Aircraft Systems

UASs continue to proliferate and may be used for nefarious activity, such as conveying physical, chemical, or biological attacks or gathering surveillance or sensitive information. The Federal Aviation Administration (FAA) estimates that the number of consumer UASs will increase from 1.9 million in 2016 to approximately 4.3 million by the end of 2020.[32] Recent known malicious use of UASs includes intrusions on large public gatherings, power infrastructure damage and outages, and radiological material delivery. Dams Sector facilities with traditionally distinct access pathways and perimeter security are susceptible to UAS intrusion because the facility security was likely not designed to address small, remotely controlled, or autonomous aircraft. Malicious UAS activity (see Figure 3) typically may be categorized as relating to surveillance, smuggling, disruption, or weaponization.

- **Surveillance:** Adversaries can use UAS video capabilities for preoperational planning to monitor and assess security operations for sensitive sites, large-scale events, and law enforcement and emergency response operations. Dams Sector facilities are more vulnerable to surveillance from UASs than threats of physical attack, as UASs present a very small physical threat compared to the size and strength of dams.
- **Smuggling:** UAS payload capabilities can be exploited to deliver illicit or contraband materials to bypass security barriers.
- **Disruption:** Adversaries can direct UASs close to a facility to access, monitor, or attack computer networks and/or monitor or interfere with radio frequency communications. Whether intentional or unintentional, UAS proximity to a facility can harass, hinder, or inhibit security operations.
- **Weaponization:** UASs can be central to an attack intended to cause casualties or physical damage; actions may include disrupting air traffic, deliberately crashing, or delivering a hazardous payload (e.g., an explosive device or a chemical, biological, or radiological weapon). Though earthen and concrete Dams Sector structures are generally not at risk from a small UAS payload weapon, ancillary facilities and adjacent open areas where people may gather could be targets of a UAS weapon.

Figure 3. *Categories and Examples of Malicious UAS Activity*
Source: DHS I&A



Vehicle Attacks

Dams Sector facilities are commonly accessible from roads and waterways, making the sector vulnerable to vehicle-borne attacks. Vehicle-borne explosives (in a car, truck, or boat) could be used in attacks, or excavation equipment could be used to damage sector infrastructure.

- **Land-Based Attacks:** Common land vehicles, such as passenger cars, cargo vans, box trucks, or semi-trailers could be loaded with explosive devices and used in attacks on Dams Sector facilities. Public roads often provide access to sector facilities or even the dams themselves, making facilities susceptible to such relatively simple attack vectors. Land vehicles could also be used in ramming attacks on crowds of people gathered at or near Dams Sector facilities (e.g., at a visitor center or in an adjacent park).
- **Water-Borne Attacks:** Similar to land-based attacks, watercraft (e.g., inflatable boats, small or large boats, personal watercraft, or barges) could be used to deliver an explosive attack on or below the water surface to Dams Sector facilities. Such vehicles could also be used in a ramming attack on infrastructure or people engaged in recreation (e.g., boating, fishing, or swimming).
- **Mechanical Attacks:** Another potential land-based attack vector is the use of mechanical equipment. Heavy or excavation equipment could be used to damage embankments or water control structures

(e.g., gates and valves), causing uncontrolled flow of water. Mechanical equipment could also be used to damage other facility structures and equipment, potentially compromising operations, safety, and security.

Case Study: Plot to Attack Hydroelectric Dams

In 2012, a Saudi national living in Texas was convicted of attempted use of a weapon of mass destruction. At the time of his arrest in 2011, Khalid Ali-M Aldawsari was researching and acquiring chemicals to make an IED. His investigations extended to identifying targets, which included nuclear power plants and hydroelectric dams; his writings included addresses for 12 reservoir dams in Colorado and California.

Aldawsari had been planning an attack for years—well before his entry into the country in 2008. He conducted online research to learn how to use chemicals to create an IED, as well as how to convert a cell phone into a remote detonator and how to booby-trap a vehicle. With the information in hand, he attempted to acquire the chemicals that comprise the IED, as well as a gas mask, a hazardous materials suit, a soldering iron kit, glass beakers and flasks, wiring, a stun gun, clocks, and a battery tester.

Fortunately, one of these purchases ultimately drew the Federal Bureau of Investigation's (FBI's) attention. Aldawsari ordered concentrated phenol, a key ingredient in the explosive trinitrophenol (TNP), and asked the shipping company to hold the package for pick-up. The shipping company returned the order to the chemical supplier and notified the police. The ensuing investigation turned up purchases of other suspicious chemicals, which led to a search of Aldawsari's residence and his arrest.

Crosscutting Issues

The Dams Sector is subject to several crosscutting issues that stem from infrastructure, social, technological, and economic changes. These include aging transportation infrastructure, dependencies and interdependencies with other sectors, and workforce issues such as decision-making errors leading to operational failures and rebuilding long-term institutional knowledge. These issues could affect multiple infrastructure sectors, increase capital expenditures, and lead to loss of life and property. Recognizing and mitigating these issues could help to limit their impacts.

Aging Transportation Infrastructure

Age and disrepair of transportation systems render most critical infrastructure vulnerable to disruptions. The Dams Sector requires secure transportation to operate effectively. The American Society of Civil Engineers 2017 Infrastructure Report Card rates United States infrastructure as a whole at D+. Of that, roads received a D; bridges, a C+; ports, a C+; rail, a B; and inland waterways, a D. This section highlights security and resilience issues for these transportation modes.[33]

Roads: The Nation's roads and highways are commonly overcrowded, in disrepair, and significantly underfunded. In 2014, over $160 billion was wasted in time and fuel owing to traffic delays and congestion. Approximately 20 percent of highways are in poor condition, causing increased costs of vehicle maintenance and repairs. An approximate backlog of over $700 billion in projects awaits funding to repair existing highways, make strategic expansions, and update the highway system (e.g., for safety, operational, and environmental improvements).

Bridges: In the United States, most highway bridges are designed for a life span of approximately 50 years. Of the more than 600,000 bridges in the United States, approximately 40 percent are 50 years old or older, and 9 percent are structurally deficient. Although bridge conditions have improved in recent years, funding for bridges may be inadequate to maintain or improve current capacities. An estimated $123 billion is needed to eliminate the Nation's bridge upgrade backlog.

Ports: The vast majority of the Nation's international trade—99 percent—flows through its ports, accounting for approximately 26 percent of its economy. As the ships carrying this cargo continue to increase in size and capacity, U.S. ports become more congested and less able to accommodate the largest ships. Ports are expected to spend approximately $155 billion from 2016–2020 to expand, modernize, and repair in response to demands of international trade. Connected infrastructure (land, rail, and inland waterway connections to ports) requires commensurate aid, yet funding for these improvements and repairs is lacking.

Rail: The freight rail industry has made important investments and repairs in the past several years to improve its systems and meet future needs. Short rail lines are in need of upgrading and maintenance funding—more so than long-distance lines—to advance in freight car size capacity and repair and replace bridges.

Inland Waterways: A total of 50,000 miles of canals, locks, and dams comprise the Unites States' inland waterways system, the majority of which is older than the original 50-year design life of its components. These waterways are an important part of freight transportation, connecting ocean ports with inland transportation hubs, accounting for approximately 14 percent of domestic freight. Age and disrepair with lack of funding result in frequent delays for hours at a time, contributing to economic losses. Although investments have been increasing in recent years, repair and upgrade projects can take decades to complete.

Dependencies on Other Sectors

Dams Sector facilities and operations are vital for assets and operations of other sectors, including Energy (e.g., hydropower), Emergency Services (e.g., emergency and firefighting water supply), Food and Agriculture (e.g., irrigation and water management), Water (e.g., potable water supply), and Transportation (e.g., inland navigable waters and roads along dams). The Dams Sector also relies on other sectors, especially Communications and Energy, to operate securely.

- **Communications:** Communications networks enable remote Dams Sector operations and control.
- **Emergency Services:** Water from Dams Sector facilities may be used by Emergency Services Sector first responders to fight fires or provide emergency water supply for other incidents.
- **Energy:** Hydropower dams provide critical electricity resources and black-start capabilities for significant portions of the Nation's power grid. Dams Sector reservoirs provide cooling water for nuclear power plants. Energy infrastructure enables hydropower facilities to move power from generation to transmission. Mine tailings are critical features to contain waste from coal extraction.
- **Food and Agriculture:** Dams Sector assets provide water for irrigation and protect farmland from flooding.
- **Transportation Systems:** Navigation lock systems in the Dams Sector enable critical inland and Intracoastal Waterway freight movements. Many major roads traverse dams.
- **Water and Wastewater Systems:** Dams Sector assets provide drinking water supplies and pumping capabilities to deliver water to other sector facilities.

Workforce Issues

Workforce issues that can affect Dams Sector security and resilience include decision-making errors influencing the severity of Dams Sector incidents, an aging workforce that will need to be replaced, and the skills gap between experienced and potential employees.

- **Decisionmaking Errors:** Human error has played a role in the compromising and failure of dams in the past and is therefore of concern for the Dams Sector. Competing social, economic, political, professional, and personal pressures—which are all human factors—can lead to erroneous decision-making and potentially cause disasters. In addition, changes in industry and regulatory standards occur over time, and engineering decisions may be made based on outdated standards. A significant example of human error relating to Dams Sector incidents is the improper management and inadequate inspection of the Ka Loko Dam in Hawaii (the emergency spillway was filled in, and inspections were not properly conducted) that led to a disastrous breach in 2006, resulting in the death of seven people.[34] Another example is the 1976 failure of the Teton Dam in Idaho caused by improperly treated foundation materials and intensified by the lack of a proper reservoir low-level outlet (the failure caused 11 deaths and $400 million in damages).[35]
- **Aging Workforce:** Many Dams Sector organizations are concerned that the average age of its workforce continues to increase and highly skilled and experienced employees are retiring, as replacing such institutional knowledge and expertise will be challenging.
- **Gaps in Skill Demand:** Coupled with the issue regarding an aging workforce, Dams Sector owners and operators are also challenged with filling the gap between the demand of skills consistent with strategic goals and the pool of potential new hires that employers find in the current labor market. Adding to Dams Sector workforce concerns is the increasing rate of personnel turnover and discrepancies between generational capabilities (personnel with decades of experience are more familiar and knowledgeable with operating manual equipment and are typically less reliant or focused on IT than newer generations).

Case Study: Wildfire Interdependency Incident

In August 2015, a lightning strike generated a wildfire near two towns that are home to a series of hydroelectric dams owned and operated by a major Seattle, Washington, utility. Sited on the Skagit River, the dams are the backbone of the Skagit Hydroelectric Project, which generates about 20% of the City of Seattle's electricity. The Goodell Creek Fire burned over 7,000 acres, damaged several electric transmission towers, and caused the temporary shutdown of the hydroelectric facilities. Debris from the fire caused transmission lines to arc, forcing the company to shut down lines connecting the Skagit complex's dams to the grid. Unable to generate and deliver power from the complex, the utility was forced to purchase replacement power from other utilities—and to source that power with about 15 minutes of warning. The loss of transmission capacity cost the utility about $100,000 per day.

One of the dams in the complex was under remote operation at the time of the fire. The fire completely cut off all access to the dam and power plant and destroyed communications and control lines to the facility. Operational control of the facility was lost until personnel could be safely flown to the facility by helicopter.

With rising temperatures and greater periods of drought, West Coast entities must face increasing fire risk. The impacted utility's power resources are 90% hydropower, so planning to protect assets such as the Skagit Hydroelectric Project is critical to the utility. Prior to the Goodell Creek Fire, the utility had already partnered with organizations such as the National Park Service, the Skagit Conservation District and its Firewise Communities program, and the Washington Fire Adapted Communities Learning Network. These partners provided valuable support and resources before, during, and after the event. The utility plans to expand its collaborations and to provide its firefighters with training focused on wildfire. Other potential mitigation actions include raising awareness of increasing wildfire risk among staff, upgrading infrastructure with fire-resistant materials, and maintaining defensible space around critical infrastructure.

Endnotes

[1] U.S. Department of Homeland Security (DHS), Dams Sector (April 2018)
[2] National Oceanic and Atmospheric Administration, Billion-Dollar Weather and Climate Disasters (January 2018)
[3] DHS and the U.S. Department of Energy, Dams and Energy Sectors Interdependency Study (April 2017)
[4] U.S. Army Corps of Engineers, Don't freak out: Dams generally do well in earthquakes (January 2016)
[5] San Gabriel Valley Tribune, What a major earthquake would do to Southern California's economy (March 2016)
[6] Office of Cyber and Infrastructure Analysis, Columbia River Basin Petroleum and Refined-Product Supplies: Disruptions and Mitigations Under Cascadia Subduction Zone Earthquake Scenario (July 2016)
[7] Central United States Earthquake Consortium, After-Action Report (September 2014)
[8] U.S. Bureau of Reclamation, Flood Overtopping Failure (November 2012)
[9] US News & World Report, The Latest: Michigan Flooding Leads to Disaster Declaration (June 2018)
[10] National Interagency Coordination Center, Total Wildland Fires and Acres (February 2018)
[11] Association of State Dam Safety Officials, State Performance and Current Issues (April 2019)
[12] Ibid
[13] Ibid
[14] American Society of Civil Engineers (ASCE), 2017 Infrastructure Report Card (March 2017)
[15] Association of State Dam Safety Officials, State Performance and Current Issues (April 2019)
[16] ASCE, 2017 Infrastructure Report Card (March 2017)
[17] Talos, New VPNFilter malware targets at least 500K networking devices worldwide (May 2018)
[18] McAfee Labs, Threats Report, (April 2017)
[19] The Register, World's biggest DDoS attack record broken after just five days (March 2018)
[20] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2016 Annual Vulnerability Coordination Report (September 2017)
[21] Symantec, Internet Security Threat Report (April 2018)
[22] Malwarebytes Labs, Cybercrime tactics and techniques: 2017 state of malware (January 2018)
[23] FBI, 2017 Internet Crime Report (May 2018)
[24] Symantec, Internet Security Threat Report (April 2018)
[25] Ibid
[26] Cisco, 2018 Annual Cybersecurity Report (February 2018)
[27] Verizon, 2018 Data Breach Investigations Report (March 2018)
[28] Cisco, 2018 Annual Cybersecurity Report (February 2018)
[29] Federal Bureau of Investigation, Quick Look: 250 Active Shooter Incidents in the United States From 2000 to 2017 (January 2018)
[30] Macrotrends, Copper Prices – 45 Year Historical Chart (July 2018)
[31] National Insurance Crime Bureau, Metal Theft Claims from January 1, 2014 through December 31, 2016 (October 2017)
[32] DHS I&A, Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges (February 2017)
[33] ASCE, 2017 Infrastructure Report Card, March 2017
[34] Hawaii Department of the Attorney General, Report of the Independent Civil Investigation of the March 14, 2006, Breach of Ka Loko Dam (January 2007)
[35] Association of State Dam Safety Officials, Case Study: Teton Dam (July 2016)

Appendix A. Resources

Key resources for this document are listed below in alphabetical order within each chapter topic. Entries without links are available from the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) website. HSIN-CI is the primary system through which private-sector owners and operators, the U.S. Department of Homeland Security (DHS), and other federal, state, and local government agencies collaborate to protect the Nation's critical infrastructure. HSIN-CI provides real-time collaboration tools including a virtual meeting space, document sharing, alerts, and instant messaging at no charge. Visit www.dhs.gov/hsin-critical-infrastructure for more information.

Natural Hazards

Central United States Earthquake Consortium, After-Action Report (September 2014) http://www.cusec.org/capstone14/documents/CAPSTONE-14_AAR.pdf

DHS and DOE, Dams and Energy Sectors Interdependency Study (April 2017) https://www.energy.gov/sites/prod/files/2017/05/f34/Dams-Energy-Interdependency-Study-508_0.pdf

FEMA, Technical Manual: Overtopping Protection for Dams (May 2014) https://www.fema.gov/media-library/assets/documents/97888

National Interagency Coordination Center, Total Wildland Fires and Acres (February 2018) https://www.nifc.gov/fireInfo/fireInfo_stats_totalFires.html

NOAA, Atlantic Hurricane Season Outlook (May 2018) http://www.cpc.ncep.noaa.gov/products/outlooks/hurricane.shtml

NOAA, Billion-Dollar Weather and Climate Disasters (January 2018) https://www.ncdc.noaa.gov/billions/overview

NOAA, National Hydrologic Assessment (Spring Flooding Outlook) (Annual, March 2018) http://www.nws.noaa.gov/oh/

OCIA, Columbia River Basin Petroleum and Refined-Product Supplies: Disruptions and Mitigations Under Cascadia Subduction Zone Earthquake Scenario (July 2016)

OCIA, Flooding and Potential Effects to Critical Infrastructure (April 2017)

State of Washington Department of Ecology, Wildfire impacts on dams: What dam owners need to know (July 2015) https://fortress.wa.gov/ecy/publications/documents/1511012.pdf

U.S. Army Corps of Engineers, Don't freak out: Dams generally do well in earthquakes (January 2016) http://usaceportland.armylive.dodlive.mil/index.php/2016/01/shakeout-dont-freak-out-dams-generally-do-well-in-earthquakes/

US News, The Latest: Michigan Flooding Leads to Disaster Declaration (June 2018) https://www.usnews.com/news/best-states/wisconsin/articles/2018-06-18/the-latest-heavy-rains-cause-rural-wisconsin-dam-failure

Technological Hazards

ASCE, 2017 Infrastructure Report Card (March 2017) https://www.infrastructurereportcard.org/wp-content/uploads/2016/10/2017-Infrastructure-Report-Card.pdf

Association of State Dam Safety Officials, State Performance and Current Issues (April 2019) https://damsafety.org/state-performance

FEMA, The National Dam Safety Program Biennial Report to the United States Congress, Fiscal Years 2014 to 2015 (August 2016) https://www.fema.gov/media-library-data/1470749866373-5de9234b8a02a3577c2646ffdf6eb087/FEMAP1067.pdf

OCIA, Aging and Failing Infrastructure Systems: Navigation Locks (December 2015)

OCIA, Impact of Population Shifts on Critical Infrastructure (July 2016)

U.S. Bureau of Reclamation, Flood Overtopping Failure (November 2012) https://www.usbr.gov/ssle/damsafety/risk/BestPractices/Presentations/IV-2-20121126-PP.pdf

Cybersecurity

Cisco, 2018 Annual Cybersecurity Report (February 2018) https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

DHS, Cloud Security Guidance (February 2018) https://www.us-cert.gov/sites/default/files/publications/Cloud_Security_Guidance-.gov_Cloud_Security_Baseline.pdf

DHS and FBI, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors (June 2017)

DHS I&A, Intelligence Assessment: Increasing Use of Ransomware May Threaten US Civilian Government and Critical Infrastructure Networks (August 2016)

DHS I&A, Likely Advanced Persistent Threat Actors Attempt Phishing Attack against South Dakota-Based Energy Company (August 2017)

Dragos, TRISIS Malware: Analysis of Safety System Targeted Malware (December 2017) https://dragos.com/blog/trisis/TRISIS-01.pdf

E-ISAC, Internet of Things DDoS White Paper (October 2016) https://nhisac.org/wp-content/uploads/2016/10/Internet-of-Things-DDoS-White-Paper-2.pdf

FBI, 2017 Internet Crime Report (May 2018) https://pdf.ic3.gov/2017_IC3Report.pdf

FireEye, Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure (December 2017) https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

ICS-CERT, 2016 Annual Vulnerability Coordination Report (September 2017) https://www.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

ICS-CERT, Advisories (multiple dates) https://www.us-cert.gov/ics/advisories

ICS-CERT, Alerts (multiple dates) https://www.us-cert.gov/ics/alerts

Industrial Internet Consortium: Industrial Internet of Things Volume G4: Security Framework (September 2016) https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

Malwarebytes Labs, Cybercrime tactics and techniques: 2017 state of malware (January 2018) https://www.malwarebytes.com/pdf/white-papers/CTNT-Q4-17.pdf

McAfee Labs, 2017 Threats Predictions (Annual, November 2016) https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

McAfee Labs, 2018 Threats Predictions (Annual, November 2017) https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/

McAfee Labs, Threats Report (Quarterly, April 2017) https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

NIST, Commission on Enhancing National Cybersecurity Report on Securing and Growing the Digital Economy (December 2016) https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

OCIA, Cybersecurity Risks Posed by Unmanned Aircraft Systems (May 2018)

OCIA, Industrial Control Systems Overview (March 2018)

OCIA, Potential Impacts of WannaCry Ransomware on Critical Infrastructure (May 2017)

OCIA, Ransomware: Goals of Malicious Actors and Current System Vulnerabilities (June 2017)

OCIA, Risks to Critical Infrastructure that Use Cloud Services (June 2017)

SANS Institute, Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017 (Annual, March 2017) https://www.sans.org/reading-room/whitepapers/analyst/cyber-security-trends-aiming-target-increase-security-2017-37702

SANS Institute, The Industrial Control System Cyber Kill Chain (October 2015) https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Symantec, Internet Security Threat Report (Annual, April 2017, 2018) https://www.symantec.com/security-center/threat-report

Talos, New VPNFilter malware targets at least 500K networking devices worldwide (May 2018) https://blog.talosintelligence.com/2018/05/VPNFilter.html

The Register, World's biggest DDoS attack record broken after just five days (March 2018) https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/

Trend Micro, New Linux Malware Exploits CGI Vulnerability (March 2017) http://blog.trendmicro.com/trendlabs-security-intelligence/new-linux-malware-exploits-cgi-vulnerability/

US-CERT, Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (March 2018) https://www.us-cert.gov/ncas/alerts/TA18-074A

US-CERT, Heightened DDoS Threat Posed by Mirai and Other Botnets (October 2016) https://www.us-cert.gov/ncas/alerts/TA16-288A

US-CERT, The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations (September 2016) https://www.us-cert.gov/ncas/alerts/TA16-250A

Verizon, 2018 Data Breach Investigations Report (March 2018) https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Criminal Activities and Terrorism

CERT, Common Sense Guide to Mitigating Insider Threats (December 2016) http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

CERT, Insider Threat Center (April 2016) http://resources.sei.cmu.edu/asset_files/Brochure/2016_015_001_452233.pdf

DHS I&A, Emerging Adversary Use of Unmanned Aircraft Systems Present Detection and Disruption Challenges (July 2015)

DHS I&A, Trend Analysis: Terrorist Incidents in the US, Canada, and Europe, May-August 2016 (October 2016)

DHS I&A, Trend Analysis: Terrorist Incidents in the West, September–December 2016 (April 2017)

DHS I&A, Unmanned Aircraft Systems Overview and Response Considerations (March 2017)

DHS IP, Mechanical Excavation Attack Vector (April 2016)

DHS Science and Technology Directorate, Cyber Security Division - Insider Threat Brochure (March 2016) https://www.dhs.gov/sites/default/files/publications/508_CSD_Insider%20Threat_Onepager_20160303_Final.pdf

DHS TSA, Vehicle Ramming Attacks: Threat Landscape, Indicators, and Countermeasures (May 2017)

DHS, Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges (February 2017) https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf

Federal Bureau of Investigation, Quick Look: 250 Active Shooter Incidents in the United States From 2000 to 2017 (January 2018) https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics

House Homeland Security Committee, Terror Threat Snapshots (December 2016, February, April 2017)

HSIN, CI SAR Reports (Multiple 2016-2017 dates)

Idaho National Laboratory, Evaluation of Unmanned Aerial Systems Threat against U.S. Critical Infrastructure (May 2017)

Institute for Economics & Peace, Global Terrorism Index 2017 (November 2017) http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf

Intelligence and National Security Alliance, Assessing the Mind of the Malicious Insider (April 2017) https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf

Macrotrends, Copper Prices - 45 Year Historical Chart (July 2018) https://www.macrotrends.net/1476/copper-prices-historical-chart-data

National Insurance Crime Bureau, Metal Theft Claims from January 1, 2014 through December 31, 2016 (October 2017) https://www.nicb.org/sites/files/2017-11/MetalTheftClaims2016Report.pdf

NCTC, Counterterrorism Digest (Weekly, multiple 2017 dates available)

OCIA, Insider Threat Behaviors and Mitigation Recommendations (March 2017)

SANS Institute, Insider Threat Mitigation Guidance (October 2015) https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307

The National Insider Threat Task Force (NITTF), Government Best Practices for Insider Threat (June 2016) https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf

Crosscutting Issues

Association of State Dam Safety Officials, Case Study: Teton Dam (July 2016) http://damfailures.org/case-study/teton-dam-idaho-1976/

Hawaii Department of the Attorney General, Report of the Independent Civil Investigation of the March 14, 2006, Breach of Ka Loko Dam (January 2007) http://the.honoluluadvertiser.com/pdf/kaloko/Kaloko-Report.pdf

Hawaii Reporter, Pflueger sentenced in Kauai dam breach tragedy that killed 7 (October 2014) http://www.hawaiireporter.com/pflueger-sentenced-in-kauai-dam-breach-tragedy-that-killed-7-people/

OCIA, U.S. Critical Infrastructure 2025: A Strategic Risk Assessment (April 2016)

Appendix B. Tools, Training, and Programs

Relevant tools, training, programs, and Dams Sector publications that may help sector stakeholders address the security and resilience issues described in this document are listed below. These resources are organized by alphabetical order within each chapter topic. This listing is not exhaustive, but it provides key resources sector stakeholders may find useful. Entries without links are available from the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Dams Portal. Visit https://www.dhs.gov/hsin-dams-portal for more information.

Natural Hazards

Dams Sector Crisis Management Handbook – The Dams Sector Crisis Management Handbook provides information relating to emergency response and preparedness issues, and includes recommendations for developing emergency action plans and site recovery plans. https://www.dhs.gov/publication/dams-crisis-management-handbook

Emergency Preparedness Guidelines for Levees – The Emergency Preparedness Guidelines for Levees provides basic recommendations regarding how to plan and prepare for high-water events and identifies some practical steps that could be considered before, during, and after such events. The document also provides some basic guidance on how to develop an emergency preparedness plan and introduces basic security concepts.

IS-324.a: Community Hurricane Preparedness – This FEMA course provides people involved in the decision-making process for hurricane preparedness with basic information about how hurricanes form, the hazards they pose, how the National Weather Service forecasts future hurricane behavior, and what tools and guiding principles can help emergency managers prepare their communities. https://training.fema.gov/is/courseoverview.aspx?code=IS-324.a

IS-325: Earthquake Basics: Science, Risk and Mitigation – This FEMA course presents basic information on earthquake science, risk, and mitigation. The course also discusses techniques for structural and non-structural earthquake mitigation. https://training.fema.gov/is/courseoverview.aspx?code=IS-325

Ready Business – The DHS Ready Business program assists businesses in developing a preparedness program by providing tools to create a plan that addresses the impact of many hazards. This website and its tools utilize an "all hazards approach" and follows the program elements within National Fire Protection Association 1600, Standard on Disaster/Emergency Management and Business Continuity Programs. https://www.ready.gov/business

Technological Hazards

American Society of Civil Engineers (ASCE) Introduction to Dam and Levee Safety – This online seminar includes a history of dams and levees and an overview of dam safety and levee criteria in the United States, identifying the consequences of failure, determining the safety of existing dams and levees, and developing techniques for rehabilitating aging dam and levee structures. https://www.asce.org/templates/conferences-events-event-detail.aspx?id=6145

ASCE Guidelines for Inspecting Earth Dams and Associated Outlet Works and Spillways – This webinar presents the key elements of typical earth dam and spillway construction as they relate to visual inspections by dam owners, public safety officials and third-party engineers. These inspections are often required by state dam safety regulations on a regular basis as part of permitting and continued operations. http://mylearning.asce.org/diweb/catalog/item/id/2264685

Association of State Dam Safety Officials (ASDSO) Awareness, Resources, and Training – ASDSO provides a variety of awareness, resources, and training to dam safety stakeholders, including federal and state dam safety professionals, dam owners and operators, engineering consultants, emergency managers, manufacturers, suppliers, academia, and contractors. https://www.damsafety.org

National Dam Rehabilitation Program – This FEMA program (as part of the National Dam Safety Program) helps local communities to rehabilitate, repair, or remove high-hazard potential dams. The program allows communities to make the preemptive investment into aging infrastructure and in the process make the communities below dams safer. https://www.fema.gov/grant-assistance-states

Cybersecurity

Cybersecurity for Small Businesses – This 30-minute, self-paced training exercise from the Small Business Administration (SBA) provides an introduction to securing information in small businesses. https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

Dams Sector Cybersecurity Capability Maturity Model (C2M2) – The Dams Sector C2M2 can help Dams Sector organizations evaluate and improve their cybersecurity programs, regardless of the type or size of the organization. https://www.dhs.gov/publication/dams-c2m2

Dams Sector C2M2 Implementation Guide – The Dams Sector C2M2 Implementation Guide is intended to address the implementation and management of cybersecurity practices associated with information technology and operations technology assets and the environments in which they operate. The document provides options for implementing the C2M2 in a systematic manner.

Dams Sector Cybersecurity Framework Implementation Guidance – The Dams Sector Cybersecurity Framework Implementation Guidance enables an organization—regardless of its size, degree of risk, or cybersecurity sophistication—to apply the principles and effective practices of cyber risk management to improve the security and resilience of its critical infrastructure. This framework recommends an approach that enables organizations to prioritize their cybersecurity decisions based on individual business needs without additional regulatory requirements. https://www.dhs.gov/publication/dams-cybersecurity-framework-implementation-guidance

Dams Sector Cybersecurity Program Guidance – The Dams Sector Cybersecurity Program Guidance outlines various strategies and methods that owners and operators can use to develop or improve a basic cybersecurity program appropriate to their cyber assets and risk profiles, including industrial control systems.

DHS Critical Infrastructure Cyber Community (C3) Voluntary Program Small and Midsize Businesses (SMB) Toolkit – To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs recognize and address their cybersecurity risks. https://www.us-cert.gov/sites/default/files/c3vp/smb/Top_SMB_Resources.pdf

Federal Communications Commission Small Biz Cyber Planner – This planner helps businesses create custom cybersecurity plans and includes information on cyber insurance, advanced spyware, and how to install protective software. https://www.fcc.gov/cyberplanner

Federal Trade Commission: Protecting Small Businesses – This Federal Trade Commission small business website helps business owners avoid scams, protect their computers and networks, and keep their customers' and employees' data safe. https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/small-businesses

Industrial Control Systems Cybersecurity Training – CISA industrial control systems program training events consist of regional training courses and workshops at venues in various locations in addition to a 5-day training event held in Idaho Falls, Idaho. https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

Internet Essentials for Business 2.0 – This guide from the U.S. Chamber of Commerce for business owners, managers, and employees focuses on identifying common online risks, best practices for securing networks and information, and what to do when a cyber incident occurs.
https://www.uschamber.com/CybersecurityEssentials

Network Security Training – CERT Network Security Training provides technical staff members, engineers, software managers, and technical leads best practices and practical techniques for protecting the security of their organization's information assets and resources. https://www.cert.org/training/

Roadmap to Secure Control Systems in the Dams Sector – This roadmap describes a plan and strategic vision for voluntarily improving the cybersecurity posture of control systems within the Dams Sector. It also highlights recommended strategies to address Sector challenges, specifies mitigation requirements, and lists long-term research and development needs regarding control system security.

Stop.Think.Connect. Toolkit – The Stop.Think.Connect. campaign has an online Toolkit that includes information specific to small and midsize businesses (SMBs). https://www.dhs.gov/stopthinkconnect-toolkit

White Paper: Every Small Business Should Use the NIST Cybersecurity Framework – This white paper from eManagement can help SMBs understand and use the National Institute of Standards and Technology (NIST) Cybersecurity Framework. It provides cybersecurity tips for SMBs aligned to the Framework's core functions: Identify, Protect, Detect, Respond, and Recover. https://cyber-rx.com/wp-content/uploads/2015/08/CyberRx-white-paper_SBs-should-use-NIST-CS-Framework_FINAL-20150804.pdf

Criminal Activities and Terrorism

Active Shooter Preparedness Program – DHS maintains a comprehensive set of resources and in-person and online trainings that focus on behavioral indicators, potential attack methods, how to develop emergency action plans, and the actions that may be taken during an incident. https://www.dhs.gov/active-shooter-preparedness

Counter-Improvised Explosive Device (IED) Awareness Products – The Office of Bombing Prevention (OBP) provides a wide array of awareness products—including cards, posters, checklists, guides, videos, briefings, and applications—that share counter-IED awareness information with the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents.
https://www.dhs.gov/counter-ied-awareness-products

Counter-IED Training and Awareness – OBP develops tools to improve national preparedness for bombing threats at all levels of government, for the public, and within the private sector. Course options include bombing prevention workshops, soft target awareness, and surveillance detection.
https://www.dhs.gov/publication/bombing-prevention-training-fact-sheet

Dams Sector Active and Passive Vehicle Barriers Guide – This guide provides information on a variety of active and passive vehicle barriers. https://www.dhs.gov/publication/dams-vehicle-barriers-guide

Dams Sector Personnel Screening Guide for Owners and Operators – This guide provides information that assists in developing and implementing personnel screening protocols.
https://www.dhs.gov/publication/dams-personnel-screening-guide

Dams Sector Protective Measures Handbook – This handbook assists in selecting protective measures addressing the physical, cyber, and human elements and includes recommendations for developing site security plans.

Dams Sector Security Guidelines – This document 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.

Dams Sector Security Awareness Handbook – This handbook assists in identifying security concerns, coordinating proper response, and establishing effective partnerships with local law enforcement and first responder communities.

Dams Sector Suspicious Activity Reporting Tool – This online tool provides Dams Sector partners with the ability to report and retrieve information pertaining to suspicious activities that may be associated with pre-operational/preparatory surveillance, activities exploring or targeting a critical infrastructure facility or system, or any possible violation of law or regulation that could compromise a facility or system and could jeopardize life or property. https://www.dhs.gov/dams-sector-suspicious-activity-reporting

Dams Sector Waterside Barriers Guide – This guide provides information on waterside barriers, including their use and maintenance. https://www.dhs.gov/publication/dams-waterside-barriers-guide

Economic Espionage Campaign – The FBI nationwide awareness campaign for economic espionage. https://www.fbi.gov/news/stories/economic-espionage

Insider Threat project – The DHS Science and Technology Directorate (S&T) Insider Threat project develops solutions that complement and expand capabilities of existing commercial insider threat tools and furthers insider threat research. https://www.dhs.gov/science-and-technology/csd-insider-threat

IS-870a: Dams Sector: Crisis Management – This FEMA course explains the application of crisis management concepts as integral components of an overall risk management program. The course provides planning guidance for Dams Sector partners to use when developing emergency action, recovery, continuity of operations, pandemic preparedness, and exercise plans.
https://training.fema.gov/is/courseoverview.aspx?code=IS-870.a

IS-871a: Dams Sector: Security Awareness – This FEMA course enhances the ability to identify security concerns, coordinate proper response, and establish effective partnerships with local law enforcement and first responder communities. The course describes common security vulnerabilities, potential indicators of threats, surveillance detection, and reporting of incidents and suspicious activities.
https://training.fema.gov/is/courseoverview.aspx?code=IS-871.a

IS-872a: Dams Sector: Protective Measures – This FEMA course addresses protective measures related to physical, cyber, and human elements and describes the importance of these measures as components of an overall risk management program. https://training.fema.gov/is/courseoverview.aspx?code=IS-872.a

IS-906: Workplace Security Awareness – This FEMA course provides guidance to individuals and organizations on how to improve the security in the workplace. No workplace—be it an office building, construction site, factory floor, or retail store—is immune from security threats.
https://training.fema.gov/is/courseoverview.aspx?code=IS-906

IS-907: Active Shooter: What You Can Do – This FEMA course provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation.
https://training.fema.gov/is/courseoverview.aspx?code=IS-907

IS-914: Surveillance Awareness: What You Can Do – The purpose of this FEMA course is to make critical infrastructure employees and service providers aware of actions they can take to detect and report suspicious activities associated with adversarial surveillance.
https://training.fema.gov/is/courseoverview.aspx?code=IS-914

IS-915: Protecting Critical Infrastructure against Insider Threats – This FEMA course provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure. https://training.fema.gov/is/courseoverview.aspx?code=IS-915

IS-916: Critical Infrastructure Security: Theft and Diversion – What You Can Do – This FEMA course introduces critical infrastructure personnel to the information they need and the resources available to them to identify threats and vulnerabilities to critical infrastructure from the theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. https://training.fema.gov/is/courseoverview.aspx?code=IS-916

Risk Assessment & Insider Threat Training – CERT Risk Assessment & Insider Threat training teaches managers, executives, security and business continuity professionals, risk managers, compliance personnel, and insider threat program managers to develop strategies for protecting their organizations from security threats and to better manage their risks. Topics covered include the CERT Resilience Management Model (CERT-RMM), OCTAVE Allegro method, and insider threat program management best practices. https://www.cert.org/training/

Spotting Insider Threats Guide – This FBI Office of the Private Sector guide defines insider threats and lists what to do when such threats are discovered. https://www.fbi.gov/file-repository/spotting-insider-threat_508.pdf

Strategic Partnership Programs – Strategic Partnership Coordinators in FBI field offices can assist business or academic institutions in protecting their technologies and preventing significant economic and national security losses. https://www.fbi.gov/file-repository/counterintelligence-strategic-partnership-programs.pdf

Suspicious Activity Reporting (SAR) Explosive Precursors Point of Sale Training – Available from the Nationwide SAR Initiative (NSI), this interactive course instructs sales personnel involved at the point of sale on behaviors and indicators that are reasonably indicative of potential terrorist and/or criminal bomb-making activity; how and where to report suspicious activity; and how to protect privacy, civil rights, and civil liberties when documenting information. https://nsi.ncirc.gov/hsptregistration/explosive_precursors/

Suspicious Activity Reporting Tool – The DHS HSIN-CI Suspicious Activity Reporting Tool allows non-uniformed law enforcement private-sector members to submit formalized suspicious activity reports and facilitate efficient information sharing and responsiveness. https://www.dhs.gov/suspicious-activity-reporting-tool

Crosscutting Issues

Critical Infrastructure Learning Series – This webinar series provides one-hour, web-based seminars conducted by critical infrastructure experts on the tools, trends, issues, and best practices for infrastructure security and resilience. https://www.dhs.gov/critical-infrastructure-learning-series

Dams Sector Information Sharing Resource Guide – This guide provides sector and cross-sector partners with information-sharing practices, products, tools, and resources that are recognized by the Dams Sector Information Sharing Environment. This information enables a more effective information exchange between government, public, and private-sector partners of the Dams Sector community.

L0260: Security and Protection of Dams and Levees – This FEMA instructor-led workshop presents information on the fundamental aspects of security and protection concepts for dams and waterways, and how these can have a substantial impact on the severity of consequences, or even prevent an incident from occurring entirely. This practical workshop provides a foundation for effective security and protection programs and provides adequate support for implementation of learned objectives outside the classroom. https://www.firstrespondertraining.gov/frt/npccatalog?courseId=2461