Dams Sector Cybersecurity Program Guidance

2016

Homeland Security

Acknowledgments

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

The *Dams Sector Cybersecurity Program Guidance* consolidates effective industry practices into a framework for owners and operators to develop and/or improve a cybersecurity program. The document is primarily intended as a resource to small and medium-sized owners and operators with varying levels of cybersecurity knowledge. However, the information may be useful to all Dams Sector owners and operators, regardless of size.

Contents

Introduction

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

The Dams Sector comprises dam projects, power plants, navigation locks, levees, mine tailings dams, industrial waste impoundments, dikes, hurricane barriers, and other water retention and water control facilities throughout the Nation. More details about the Dams Sector can be found in the *Dams Sector-Specific Plan and Dams Sector Roadmap to Secure Control Systems*.

Dams Sector Cybersecurity Program Guidance (guidance) consolidates effective industry practices into a framework within which owners and operators can develop and/or improve a cybersecurity program. The security of control systems—including both internal and external processes and business systems—promotes the protection of systems and data, public safety, and public confidence. The industry practices included in this guidance—tools, methodologies, guidelines, and frameworks—are consistent with provisions included in the cybersecurity-related documents listed in Appendix G. Source Documents, including:

- Dams and Energy Sector documents related to cyber and information security
- Federal agency guidelines from the Federal Energy Regulatory Commission (FERC), National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation (NERC), U.S. Department of Energy (DOE), and U.S. Department of Homeland Security (DHS)
- NIST Special Publications: Computer Security and Cybersecurity Practice Guides

Primary Elements of a Cybersecurity Program

Cybersecurity program planning and implementation, in addition to enhancing the security of an organization's cyber assets, can enable owners and operators to support the national effort to improve control system security throughout the Dams Sector. An effective cybersecurity program combines cyber systems, policies, and procedures into a common framework to address cyber risk. Fundamental elements of an effective cybersecurity program include:

- **Cyber asset identification** provides the starting point from which owners and operators select and apply security measures to protect and reduce the risk to those assets. Identifying cyber assets and determining their criticality positions owners and operators to conduct cybersecurity assessments and improve an organization's security posture. Many tools developed by the Dams Sector or by Federal agencies are available to help sector owners and operators identify critical assets.
- **Cybersecurity assessments** enable owners and operators to identify cybersecurity risks and evaluate the organization's cybersecurity practices and cyber-operational resilience. Such assessments improve an owner's or operator's understanding of their cybersecurity posture, vulnerabilities, and what actions are needed to address them. Several cybersecurity risk assessment tools are available, many of which are offered at no cost to owners and operators.

- **Cybersecurity risk management** is necessary to protect assets and to address the ongoing process of identifying, assessing, and responding to each of the elements of cyber risk (i.e., threat, vulnerability, and consequence). Comprehensive cybersecurity risk management entails understanding cybersecurity posture and target state, identifying and prioritizing security measures, assessing progress, and communicating cybersecurity risk. Several cybersecurity guidelines can be consulted in order to develop a risk management plan and clearly-defined security policies, standards, and measures.
- **Response and recovery** procedures (e.g., incident response and continuity of operations) represent core functions of the most basic cybersecurity program. Once in place, these procedures enable owners and operators to prepare for and respond to an incident, maintain resilience, and restore disrupted capabilities or services.

How to Use Dams Sector Cybersecurity Program Guidance

Dams Sector Cybersecurity Program Guidance outlines various strategies and methods to develop or improve a basic cybersecurity program, enabling owners and operators to select cybersecurity activities and measures appropriate to their cyber assets and risk profile. Each chapter of the guidance focuses on a distinct element of a basic cybersecurity program—identify assets, assess risk, manage risk, and respond and recover. Industry-recognized best practices and means by which to obtain additional information are also included.

This guidance is primarily designed to help owners and operators with small- and medium-sized electricity production and water management assets to develop and/or improve a cybersecurity program. However, all Dams Sector owners and operators, regardless of size or asset function, may find the information useful. A sequential review of this document can help owners and operators develop and implement a cybersecurity program appropriate for their facilities' cyber risk profiles, operational processes, business environments, regulatory requirements, and available resources.

Disclaimer

Dams Sector Cybersecurity Program Guidance is not intended to supersede, modify, or replace any existing laws, regulations, codes, standards, or policies applicable to the sector. Regulatory agencies may require compliance with or override portions of this guidance. The publication of this guidance does not constitute endorsement of any product or product type, nor does it test, certify, or approve any products. The use of this guidance is entirely voluntary.

In addition, complete cybersecurity is never fully achievable. The overall level of cybersecurity will vary in accordance with site-specific conditions and specific threats to each individual cyber asset. Each owner or operator must decide the level of risk that is considered practical and acceptable, as well as the corresponding cybersecurity practices deemed acceptable.

1. Asset Identification

Identifying an organization's cyber assets—including critical cyber assets—is the starting point from which owners and operators design a cybersecurity program. Owners and operators should review their organization's assets to identify and inventory critical and noncritical cyber assets, taking into consideration business value and applicable regulations. After identifying cyber assets and determining their criticality, owners and operators can conduct cybersecurity assessments to determine where system vulnerabilities exist and what actions are needed to address them. Risk mitigation measures may then be applied to improve an organization's cybersecurity posture, prevent or mitigate a cyberattack, and ensure the continuity of facility operations and services.

This guidance provides a comprehensive approach with recommended strategies to identify and determine criticality of cyber assets and systems. The approach includes:

- Identify cyber assets by locating and creating an inventory of all network infrastructure, devices, applications, data storage, data flows, and network connections. Consider the roles and functions of the assets, as well as associated assets that support their operation, for their potential impact on cyber systems as a whole.
- Determine the degree of criticality of the identified assets using existing Dams Sector and other Federal agency guidance documents (such as from FERC, NERC, and the Transportation Security Administration (TSA)). Owners and operators may also develop their own frameworks, policies, procedures, or considerations for determining cyber asset criticality based on existing guidance.

Cyber Asset Classification

Cyber Systems are any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services (e.g., business systems, control systems, and access control systems).

Cyber Assets comprise data and interconnected or non-connected hardware and software components (e.g., computers, database, applications, and control and monitoring devices) that together perform a particular function or interrelated set of functions.

Critical Assets are those facilities whose destruction or compromise would result in a high-consequence event (i.e., significant long-term negative consequences, such as loss of life, adverse public health and safety, economic hardship, or a damaging psychological effect on the Nation).

Noncritical Assets are those cyber assets that are not essential to life safety and/or functionality objectives.

Cyber Asset Identification

Cyber systems in the Dams Sector include business systems, control systems, access control, and other specialty systems. Owners and operators can develop internal tools, such as asset identification templates, as mechanisms to efficiently identify and inventory their cyber assets. In addition, such criteria can be used to standardize how to determine the criticality of cyber assets, as outlined in the next section.

The roles and functions that the cyber systems serve can impact the reliable operation of critical functions. When identifying cyber systems, consider the following types of critical functions:

- Provides operation information in real-time
- Controls manual or automated parameters
- Calculates parameters or limits
- Generates or displays prompts or alarms
- Provides connectivity between cyber systems
- Supports continuity of operations for the critical functions or local recovery plans

In addition to identifying critical functions, cyber asset identification can take into account secondary or supporting cyber systems whose loss, degradation, or compromise could impact both the operation of critical cyber systems and their associated critical functions. This identification is based upon whether a failure or compromise of these assets would affect the safety, reliability, functionality, and/or performance of cyber systems and would lead to issues with safety and/or reliability of a Dams Sector asset. Secondary or supporting systems may include:

- Assets that facilitate the recovery and restoration process such as generators, spare parts, and spare systems
- Stand-alone virus and malware scanners; archival, backup, and restoration systems; and log monitoring systems (except for cyber assets used in the access control and/or monitoring of logical and/or physical security zones)
- Environmental systems such as heating, ventilation, and air conditioning (HVAC)
- Support systems such as uninterruptable power supplies and alarm systems
- Cyber systems supporting value chain activities

Additional information on cyber systems is located in Appendix B. Types of Cyber Systems.

Cyber Asset Criticality

The next step after compiling the inventory of the organization's cyber assets is to identify which assets are "critical." It is not possible to provide absolute security for all facets of a facility. Therefore, organizations should identify all assets, prioritize the most important assets, and provide the best level of protection for the important assets commensurate with the discernible risk. Taking into consideration new technologies, systems, and software, regular review and updating of the critical cyber asset inventory (e.g., annually or when new equipment is procured) can help owners and operators anticipate potential cyber risks. This section presents a methodology for identifying critical assets based on set criteria and assessment of the asset's impact on safety and security. The sector-specific and Federal guidelines included in this chapter provide additional information on other methodologies for determining criticality.

Dams Sector Mission Critical Functions

Executive Order 13636 initiated the Cyber-Dependent Infrastructure Identification Working Group, which called for the identification of sector-specific mission critical functions. In 2013, the Dams Sector-Specific Agency identified the sector's critical infrastructure at greatest risk: critical cybersecurity functions and services, associated value chains, and supporting cyber infrastructure.

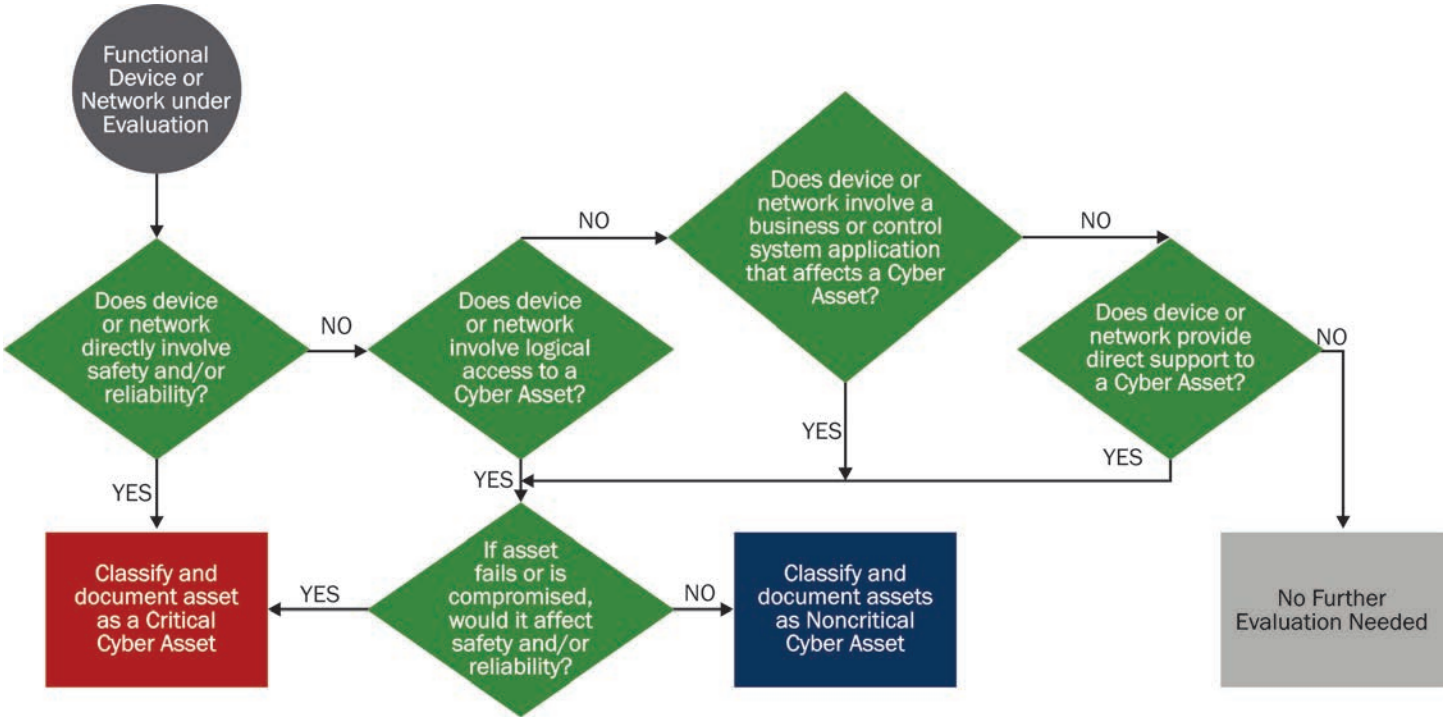
These risk factors are important to consider when determining cyber asset criticality:

- How the compromise or loss of a particular asset impacts the owner's or operator's ability to perform the activities associated with its mission critical functions (e.g., flood control, water supply, navigation, recreation, transport of power, and hydropower generation).
- How documenting and evaluating the threats, vulnerabilities, and consequences related to a loss or compromise of cyber assets will help in developing a risk management strategy to protect those assets.
- Whether business operations or plant operations are being evaluated.
  - **Business Operations:** Assets are often categorized as Mission Critical, Mission Essential, Business Core, or Business Supporting.
  - **Plant Operations:** Critical Cyber Assets are those where a failure or compromise of these assets would affect the safety, reliability, functionality, and/or performance of cyber systems that would lead to issues with the safety and/or reliability of the asset.

Criticality Determination

Criteria to determine critical and noncritical cyber assets or systems (i.e., a group of cyber assets) is based on the evaluation of the asset as essential or nonessential to operations and the degree to which loss, degradation, or compromise of the asset impacts safety and/or reliability of operations. As outlined in Figure 1, this process evaluates a functional device or network based on its involvement with (1) safety and/or reliability, (2) logical access to a cyber asset, (3) business systems or control system application, or (4) a supporting asset providing direct support to a cyber asset. Assets with direct involvement with safety and/or reliability are immediately determined to be critical. If the functional device or network involves one of the remaining three qualifications, it is further evaluated for the impact of its failure or compromise on safety and/or reliability. The result is that assets are organized into three categories: Critical Cyber Asset, Noncritical Asset, and No Further Evaluation Needed.

Figure 1. Criticality Assessment Flow



Critical cyber assets or critical cyber systems refers to those that are essential to the safety and/or reliability objectives of the facility. Cyber systems that a facility may wish to consider critical to operations include:

- A control system (including a remotely operated control system) that directly monitors and/or controls electricity production, water management, or other physical processes
- An access control or security monitoring system that is connected to other systems
- A system used to transmit sensitive information (e.g., e-mail, facsimile, file transfer protocol) regarding the status, operation, or protection of an asset(s)
- A noncritical control system on the same network as a critical control system
- A watchdog system (e.g., Safety Instrumented System) for a critical control system
- A system hosting critical or sensitive information (e.g., personally identifiable information, facility plans) that, if exploited, could result in the cyber sabotage of its processing or control capabilities

Noncritical cyber assets or noncritical cyber systems refer to those systems that are not essential to the safety and/or reliability objectives of the facility. Cyber systems that a facility is unlikely to consider critical to operations include:

- A control system that is not connected to any critical systems
- A headquarters business system that contains no sensitive information
- A financial system for the facility or organization

Assets falling into neither category need not be evaluated any further from a criticality standpoint. However, the owner or operator may protect the assets for other reasons, as dictated by the facility's risk profile.

Criticality Determination Guidance Documents

Many tools are available to help sector owners and operators identify critical assets. The tools include common guidelines by which sector owners and operators may identify and prioritize their portfolios of critical assets:

- **Dams Sector Consequence-Based Top Screen (CTS) Methodology** can help sector owners and operators with multiple facilities to identify, assess, and prioritize critical assets. The purpose of the CTS methodology is to identify critical assets within the Dams Sector at the portfolio level (e.g., owner, State, regional, and national).
- **FERC Division of Dam Safety and Inspections *Security Program for Hydropower Projects*** provides guidelines for identifying critical cyber assets based on criteria relating to two potential consequences: (1) the unintentional release of all or part of the reservoir's contents affecting the downstream population and infrastructure and (2) non-operation of a licensed facility resulting in a loss of significant power generation. A cyber asset's criticality is based on the exceedance of FERC-specified consequence threshold values, and will determine the level of security measures (baseline or enhanced) to be implemented.
- **NERC *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** provides a methodology for identifying cyber assets that are essential to the reliability or operability of the facilities and control systems necessary for operating an interconnected electric energy transmission network. For the Dams Sector, this is directly relevant to hydropower facilities and assets; yet the NERC guideline may also be relevant and beneficial for other portions of the sector.
- **TSA *Pipeline Security Guidelines*** provides a simplified process to determine facility and asset criticality, which may be more appropriate for owners and operators without an extensive, multisite portfolio of assets. Owners and operators are encouraged to determine facility criticality based on criteria indicating the severity of potential impacts resulting from that facility's damage or destruction.

Further information on these tools and their application to critical asset identification can be found in the *Dams Sector Security Guidelines*.

2. Cybersecurity Assessments

The keys to robust cybersecurity are conducting assessments to identify cybersecurity risks and evaluating an organization's cybersecurity practices and cyber-operational resilience. By conducting cybersecurity assessments, owners and operators can determine their cybersecurity posture, including where system vulnerabilities exist and what actions are needed to address them. Assessments empower owners and operators to prevent or mitigate the consequences of a cyberattack, such as equipment damage, loss of hydropower generation, damage to major dam infrastructure components, or manipulation of the infrastructure. Cybersecurity assessments may be conducted as self-assessments or by third-party cybersecurity professionals.

Assessment Factors for Cyber Risks

Threat: Malicious or unintentional damage or disruption of cyber asset(s) that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability: Physical feature or operational attribute that renders a cyber asset open to exploitation or susceptible to a given threat.

Consequence: Effect or impact of an event, incident, or occurrence.

This guidance provides a comprehensive approach and recommended strategies for conducting cybersecurity assessments in order to increase the security of control systems and associated information across the Dams Sector. The approach includes:

- Identify potential threats to control systems and associated information
- Develop an understanding of common vulnerabilities and potential consequences
- Use assessment tools and methodologies to identify practical risk management solutions
- Promote information sharing and improve sector-wide awareness of cybersecurity concerns

Cybersecurity Risk Assessment

Risk is understood as the probability of an undesirable event occurring, or the capacity for a potential loss and its probability of occurrence. Assessing risk entails identifying the undesired event or consequence and the probability of its occurrence, which includes examining threats and vulnerability. Owners and operators are encouraged to perform ongoing risk assessments (e.g., vulnerability assessments) of their cyber assets and systems and understand the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Ultimately, effective risk assessments help owners and operators to identify risk management solutions tailored to address vulnerabilities; meet specific security, business, and operational requirements; and prioritize the investments needed to support these solutions. Sample solutions and frameworks are included in the next chapter, Cybersecurity Risk Management.

The five steps of a risk assessment are:

- Identify threat sources relevant to organizational information systems and events that could be produced by those sources.
- Identify vulnerabilities that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation.
- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful.
- Determine the magnitude of impact (consequence) to organizational operations and assets, individuals, other organizations, and the Nation.
- Determine risk as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

The impact of a cyber incident on a control system(s) may encompass both physical and digital functions. Organizations should therefore consider the potential consequences resulting from an incident on a control system. The risks may be safety-, health-, compliance-, functionality-, reputation-, or environment-related rather than purely economic. Cyber incidents can also generate consequences for another organization's infrastructure (e.g., a downstream water treatment plant and neighboring jurisdictions). The risks may result in an unrecoverable consequence rather than a temporary financial setback. Well-defined policies, standards, and procedures lead to mitigation techniques designed to thwart incidents and minimize the consequences to manage the risk. Additional considerations when conducting a risk assessment on a control system include:

- Impacts on safety and use of safety assessments
- Physical impact of a cyber incident on a control system (including the larger physical environment), effect on the process controlled, and the physical effect on the control system itself
- The consequences for risk assessments of mechanical components within a control system

Assessment Tools and Methodologies

Several cybersecurity risk management tools, processes, standards, and guidelines are available that may align well with the NIST *Cybersecurity Framework* (Framework) security and risk management approaches and help demonstrate how an owner or operator is already applying Framework concepts. Effective and accepted cybersecurity assessment tools include:

- **Dams Sector Cybersecurity Capability Maturity Model (C2M2)**, to be released in 2016, is a no-cost, voluntary tool utilizing industry-accepted cybersecurity practices to assess an organization's cybersecurity capabilities and prioritize actions and investments to improve their cybersecurity posture. C2M2 supports the adoption of the NIST *Cybersecurity Framework* and also assesses domains similar to that of the Cyber Resilience Review (see below).
- **Cybersecurity Risk Assessment (CRA)** is the process of collecting information and assigning values to cyber risks so informed decisions can be made pertaining to the management and mitigation of those risks. Particularly within critical infrastructure, owners and operators should understand the likelihood and the potential impact of a cyber event. With such information, owners and operators can determine the acceptable level of risk, which is also known as their risk tolerance. By understanding their risk tolerance, owners and operators can prioritize cyber risks that may require mitigation. A CRA provides the ability to identify cyber risks, determine threats, assess vulnerabilities and potential consequences on a continual basis, and assist the decision-maker in making cost-effective investments in risk mitigation. It is also important to reassess the risks as threat conditions change.
- **Cyber Resilience Review (CRR)** is a no-cost, voluntary, non-technical assessment offered by DHS that is designed to evaluate an organization's cyber-operational resilience and cybersecurity practices across 10 domains. Although the CRR predates the NIST *Cybersecurity Framework*, most of the assessed CRR practices align closely with the Framework. The CRR can be used to evaluate the resilience capabilities of enterprises with highly defined and mature operational resilience capabilities, as well as organizations with less defined and mature capabilities. Owners and operators can also choose to download the free self-assessment or schedule an onsite assessment facilitated by trained DHS cybersecurity professionals; both options generate a final report inclusive of options for consideration and the organization's maturity level relative to the assessed domains.
- **Cyber Security Evaluation Tool (CSET)** is a no-cost, desktop software tool offered by DHS that guides users through a step-by-step process to assess their control systems and IT network security practices against recognized industry standards. The user selects one or more of the government- or industry-recognized cybersecurity standards, and the tool generates assessment questions specific to the selected requirements. The tool then compares answers with the recommended requirements from the standards selected. After completion of the assessment, the tool generates a prioritized list of recommendations for improving the organization's cybersecurity posture and associated actions to be taken.

- **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Assessment Program** works with owners, operators, vendors, integrators, and government agencies to assess various aspects of critical infrastructure (e.g., cybersecurity controls, control system architectures, and adherence to best practices) and provides options to mitigate and manage risk. Core assessment products and services include self-assessments using CSET, onsite field assessments, network design architecture reviews, and network traffic analysis and verification. The products improve situational awareness; provide insight, data, and identification of control systems threats and vulnerabilities; and provide the context necessary for enhancing cybersecurity.

Cybersecurity Information Sharing

Successful cybersecurity practices rely on regular, timely, and accurate threat, vulnerability, and consequence information. Given the changeable nature of risk information, particularly threat information, owners and operators rely on a reliable, steady stream of information to protect cyber assets, systems, networks, and functions by making informed decisions about short- and long-term cybersecurity posture, risk mitigation, and operational continuity. Robust information-sharing practices incorporate both internal (within the organization) and external (sector-wide) sharing of information.

The following cyber information-sharing mechanisms are available to Dams Sector owners and operators:

- **ICS-CERT** collaborates with both government and industry to improve the cybersecurity posture of control systems within the Nation's critical infrastructure. Resources available through ICS-CERT assist owners and operators to report control system security incidents or software vulnerabilities and to develop sound mitigation strategies that strengthen their cybersecurity posture and reduce risk. Information products are available to owners and operators through the ICS-CERT Website or by subscribing to the organization's alerts. Examples include Advisories (timely information about current cybersecurity issues, vulnerabilities, and exploits) and Alerts (timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks).
- **Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Dams Portal** is a trusted, Internet-based information-sharing network that allows sector partners to collect and disseminate information among Federal, State, and local agencies, as well as the private sector. The Dams Portal on HSIN-CI is the primary information-sharing mechanism for the Dams Sector. The portal enables owners and operators to share suspicious activity reports, research documents related to Dams Sector security and protection, access training products, and receive information on emerging threats and incidents (including from ICS-CERT).
- **FBI InfraGard** is a partnership between the Federal Bureau of Investigation (FBI) and the private sector that is dedicated to sharing information and intelligence to prevent hostile acts against the United States. Each InfraGard Members Alliance is geographically linked with an FBI Field Office, providing all stakeholders immediate access to experts from law enforcement, industry, academic institutions, and other government agencies. Utilizing the talents and expertise of the InfraGard network to share information mitigates threats to the Nation's critical infrastructure.
- **Security Intelligence Feeds** enable owners and operators to gather, share, and validate relevant, timely, and accurate information about new or ongoing cyberattacks and threats. Vendors provide no-cost or fee-based services: basic, no-cost versions generally provide access to open source daily newsletters and facilitate connections between security professionals, while fee-based services include full intelligence reports, customizable alerts, and tools to aid in investigations.

3. Cybersecurity Risk Management

A cybersecurity risk management program provides an effective method to protect cyber assets (e.g., systems, data, information, and networks) and encompasses the ongoing process of identifying, assessing, and responding to each of the elements of cyber risk (i.e., threat, vulnerability, and consequence). In implementing a cybersecurity risk management approach, an owner or operator begins by identifying risks and then proceeds to develop a risk management plan and implement clearly defined cybersecurity policies, standards, and procedures to detect, respond, and recover from incidents generated by those identified risks.

Several guidelines are available to owners and operators to develop a comprehensive cybersecurity risk management program. Owners and operators should first implement cybersecurity requirements dictated by law and regulation; the guidelines in this chapter can then be used to identify and implement additional measures. This guidance provides a comprehensive approach with recommended strategies that may be used to implement a new cybersecurity risk management program or to build on an existing program. By utilizing various cybersecurity risk management strategies applied throughout the Dams Sector, organizations, regardless of size or structure, can apply nimble, flexible risk management strategies to improve the security and resilience of their critical infrastructure. Such strategies include:

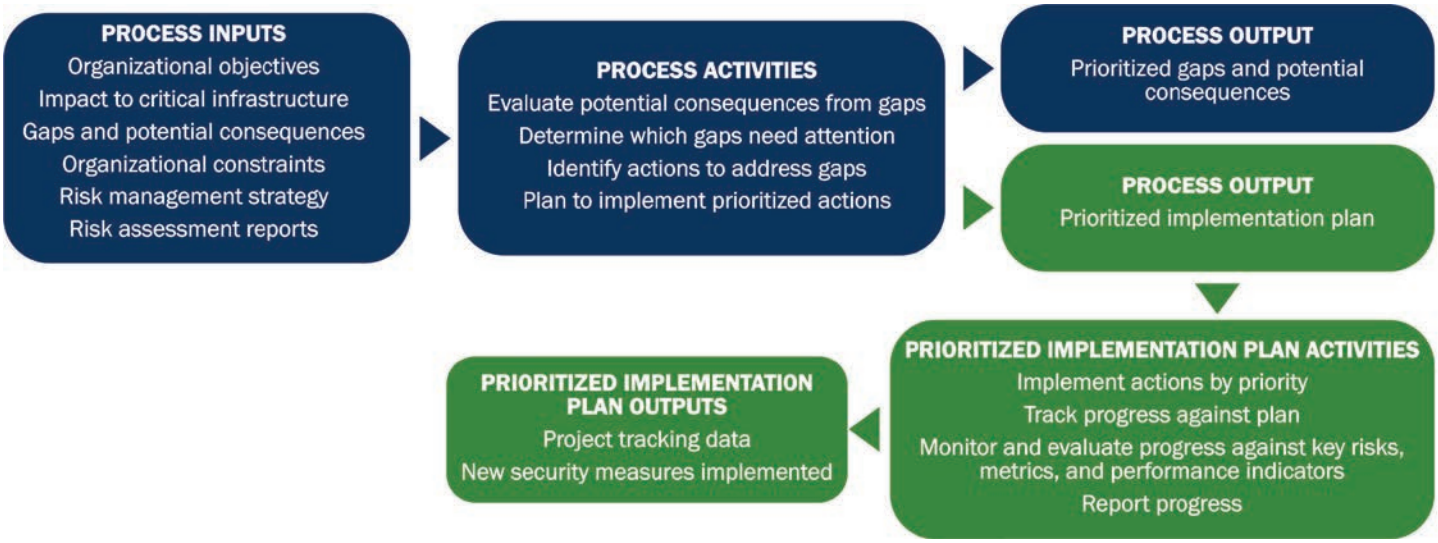
- Understanding of the organization's current cybersecurity posture and targeting a future state that reflects desired outcomes
- Identification and prioritization of opportunities for reducing cybersecurity risk
- Assessment of progress toward the target cybersecurity state
- Communication among internal and external stakeholders about cybersecurity risk

Risk Management Plan

Self-evaluation of cybersecurity risk management practices is integral to meeting or exceeding an organization's cybersecurity goals as the results are leveraged to inform and implement a cyber risk management plan. This enables owners and operators to identify current cybersecurity risk management practices, map these practices to specific levels of maturity and set targets, and identify potential gaps and practices to advance cyber risk management. It is important to note that determining where to apply cybersecurity capabilities (based on vulnerabilities), identifying the current cybersecurity and risk management state, and performing a risk assessment are important activities to building an informed risk management plan.

The risk management steps illustrated in Figure 2 help organizations to create a cyber risk management plan that identifies possible risk mitigations or other measures to address identified risks. Process activities leading to the development of a plan are indicated by blue text, and activities to implement the plan are in green text. The owner or operator begins with inputs, such as organizational objectives, that are used to conduct the risk management activities. The final stage in the risk management process (under "outputs") is to implement the chosen cybersecurity risk response by establishing a cyber risk management plan (or strategy). The plan can account for the unique nature of the owner's or operator's cyber infrastructure by specifying the implementation strategy. The plan can also identify milestones and activities to be used to guide, measure, and inform cyber risk management decisions. The owner or operator executes the plan and tracks its progress over time, ensuring that gaps are closed and risks are monitored. Complete steps for conducting a self-evaluation and benefiting from the results are included in the *Dams Sector Cybersecurity Framework Implementation Guidance*.

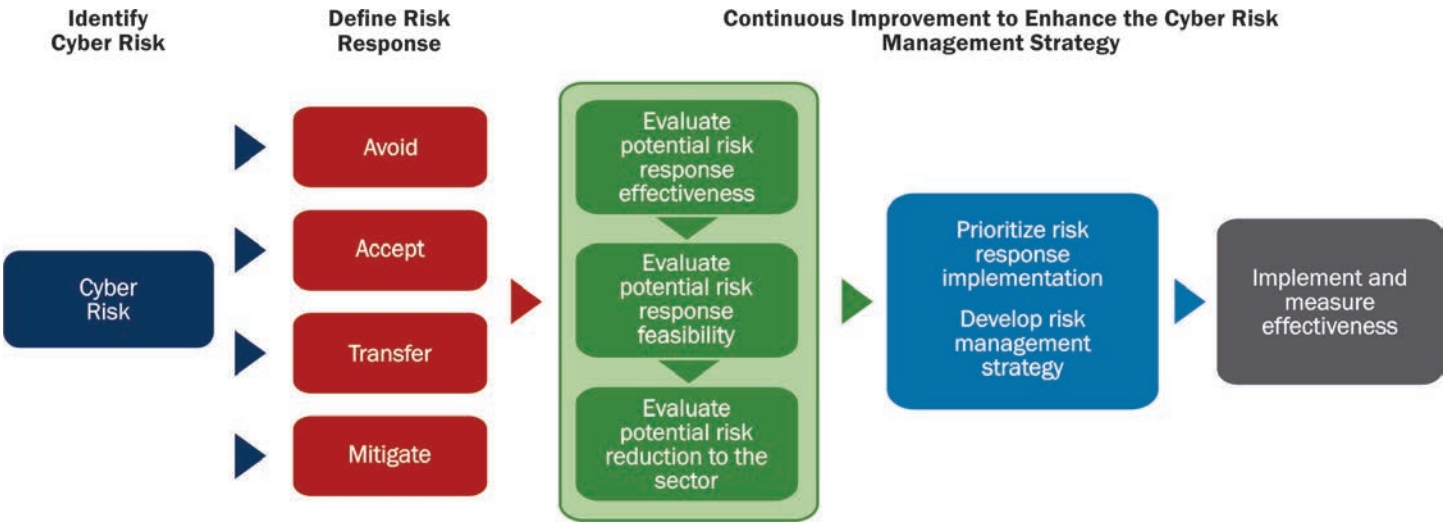
Figure 2. Risk Management Planning



Risk Management Strategies

Risk management is the course of action taken in order to manage risk; essentially, how an organization chooses to respond to risk. Once the organization understands the risk, such as through threat information or a risk assessment, risk management responses are defined and prioritized. Prior to making a decision, the organization should understand the cyber risk to organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals. There are four commonly used cyber risk management strategies: avoid, accept, transfer, and mitigate. As depicted in Figure 3, owners and operators may choose to remove the exposure to risk (avoid), not take action (accept), shift some or all of the risk to another asset/area (transfer), or apply measures to reduce event likelihood or consequences (mitigate). In order to consider these four options in a comparable way, the approach provides a process through which owners and operators can discuss and evaluate various factors that help determine the appropriate cyber risk management response. Continuously evaluating the risk management strategy—such as measuring the effectiveness of a selected risk response—ensures that implemented strategies are responsive to the risk environment and effectively address the cyber risk environment.

Figure 3. Overview of Risk Management Approach



The primary elements of the decision process are important to consider when deciding which risk management response to implement:

- Evaluating the effectiveness of a particular risk response: How much risk is reduced by this response?
- Evaluating the feasibility of implementing the risk response: Are there obstacles to implementing the risk response? If so, how significant are they?

Cybersecurity Functions

A comprehensive approach to cybersecurity typically will involve clearly defined policies, standards, and procedures that address all cyber systems used by an asset, with certain enhanced security activities directed at critical systems.

To assist in developing policies, standards, and procedures, owners and operators are referred to the most current versions of the NIST Special Publication (SP) 800 series documents, in addition to the most current versions of regulatory agencies' cybersecurity documents (e.g., FERC/NERC Critical Infrastructure Protection (CIP) standards). The NIST SP 800 series focuses on computer security and contain computer, cyber, and information security guidelines, recommendations, and reference materials. The NIST SP 1800 subseries complements the SP 800 series, focusing on practical, user-friendly guides for adoption of standards-based cybersecurity approaches. NERC's FERC-approved CIP reliability standards address the security of cyber assets and cover a range of cybersecurity areas. While these source documents vary in their use of cybersecurity functions, measures, and controls, this guidance introduces several common terms useful in the development of a cybersecurity program.

Policies, Standards, and Procedures

Security Policies:

- Instructions indicating the organization's intentions about its information technology operations
- High-level statements providing guidance that does not generally change as technology evolves
- Generalized and broadly scoped legal statements

Security Standards:

- Statements that make specific mention of technologies, methodologies, and other detailed factors affecting the operation of information system resources
- Statements that are flexible and change as technology evolves
- Statements with scope limited to a specific technology (e.g., Wi-Fi, desktop personal computers, servers)

Security Procedures:

- Adoption of a standard
- Implementation of an ordered set of tasks to perform a specific action
- Uniform execution of a set of actions or operations in order to consistently obtain the same result under the same circumstances (e.g., Data Backup Procedure)

Baselining

Baselining includes creating a detailed inventory—at a point in time—of infrastructure components, configurations, and services necessary for steady-state control systems operation. Whereas the identification and criticality determination of assets described in Chapter 1. Asset Identification is performed on a broad scale (e.g., facility or enterprise level), baselining involves inventorying components, configurations, and services on a much smaller, granular scale.

Baselining commonly includes information about control system components, network topology, and the logical placement of those components within the system architecture. Examples of control system components include standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings or parameters. Maintaining a current system baseline improves an owner's or operator's understanding of control system performance and helps to identify risks when conditions deviate from the baseline. Effective baselining practices include:

- Document control system components and configuration during a known secure, steady state to determine system performance and identify proper operating conditions
- Track the control system over time to identify anomalies or unexpected changes relative to the baseline (e.g., undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes)

- Apply procedures (e.g., security measures or information system security controls described below) to address system anomalies or changes discovered
- Create new baselines as control systems change over time, or at routine system backup intervals (e.g., hourly, daily, or weekly)

For additional information on baselining, see *Guide for Security-Focused Configuration Management of Information Systems* (NIST 800-128) and *Guide to Information Technology Security Services* (NIST 800-35).

Security Measures

Cybersecurity measures are specific actions taken in alignment with cybersecurity policies, standards, and procedures. After identifying cyber assets and determining their criticality, owners and operators conduct cybersecurity assessments to better understand their cybersecurity posture, where system vulnerabilities exist, and what actions are required to address them. Taking into account assessment results, specific cybersecurity measures are then designed and applied. Applying cybersecurity measures enables organizations to address known risks and vulnerabilities, improve their cybersecurity posture, prevent or mitigate a cyberattack, and ensure the continuity of facility operations and services.

When implementing cybersecurity measures, an owner or operator may choose to only implement measures to address select deficiencies. However, given the evolving cyber landscape, owners and operators may best improve their cybersecurity posture through the implementation of comprehensive cybersecurity risk management measures across the cybersecurity Functions: identify, protect, detect, respond, and recover. Security measures are then applied based on the criticality of the asset:

- **Noncritical cyber assets:** apply baseline security measures
- **Critical cyber assets:** apply baseline and enhanced security measures

Lists of baseline and enhanced security measures can be found in Appendix C. TSA Baseline and Enhanced Security Measures. Additional information on assessments can be found in Chapter 2. Cybersecurity Assessments.

Information System Security Controls

Security controls are the managerial, operational, and technical safeguards or countermeasures employed within an organizational system to protect the availability and integrity of the system and its information. They are commonly organized into three main categories (i.e., administrative, technical/logical, and physical) and can be applied before an incident (e.g., preventive controls such as firewalls or security awareness training), during an incident (e.g., detective controls such as system monitoring or intrusion detection systems), or after an incident (e.g., corrective controls such as system upgrades or vulnerability mitigation). Security controls may also include physical access control measures, such as cameras, secure keys, and physical access devices.

An effective cybersecurity program includes a combination of categories of information system security controls:

- **Administrative controls** are the laws, regulations, policies, practices, and guidelines that govern the overall requirements and controls for a system security program. Administrative controls may include developing/disseminating policies, standards, or procedures; creating disaster preparedness or recovery plans; screening personnel; or separating/segregating duties (e.g., one individual cannot control all key aspects of operations—more than one person is required to complete a task).
- **Technical/logical controls** are technologies that control information system access and the usage of both the system and its sensitive information. These controls are far-reaching and exercise control throughout a physical structure or over a network. Technical/logical controls may include encryption, identification and authentication methods, firewalls, anti-virus software, and maker/checker applications (relating to the administrative control of separating duties).

- **Physical controls** are measures that deter or prevent unauthorized access to the system and its sensitive information. For example, whereas a firewall requires a technical/logical key to obtain access to a network, a physical, locked door requires a physical key to access a sensitive room. Addressing cyber-physical dependencies is critical, as control systems can be compromised and manipulated to operate equipment in such a way as to cause damage and inflict onsite and offsite causalities. Physical controls may include video surveillance systems, lighting, gates and barricades, security guards or other personnel used to regulate access to an office, and remote backup facilities.

As the risk to a system's confidentiality and integrity increases, so too does the need for additional security controls. Selecting the appropriate set of security controls improves the day-to-day operations of the organization and helps to accomplish the organization's stated missions and business functions. NIST SP 800-53 provides a comprehensive catalog of security and privacy controls for information systems—including administrative, technical/logical, and physical control types—and is a starting point for selecting additional security controls. Owners and operators can use this guidance to tailor security controls to each organization's specific needs, based on their mission, operations environment, and technologies used. Ensuring the security of control systems is critical as dams employ a variety of infrastructure to monitor, automate, and manage critical physical processes. NIST SP 800-82 provides ICS-tailored security controls based on NIST SP 800-53, in addition to identifying known threats and vulnerabilities to these systems and recommended countermeasures.

For additional information on security controls, see Appendix D. Cyber and Physical Security Measures for Dams Sector Owner and Operators, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST 800-53), and *Guide to Industrial Control Systems (ICS) Security* (NIST 800-82).

Vendor Security

The environments in which control systems and IT systems operate are constantly changing and can encompass supply chain relationships and procurement/acquisition processes. In addition, information systems (including system components) need to be protected throughout the system's life. Owners and operators should be aware of the threats and vulnerabilities introduced by vendors along the supply chain, such as being cognizant of necessary updates to firmware and software.

Embedding cybersecurity in the procurement of Dams Sector systems is an important step for safeguarding sector infrastructure. It ensures that those supplying products and services (e.g., software, systems, maintenance, and networks) consider cybersecurity principles and controls when designing those products and services. Moreover, cybersecurity risk can be reduced by asking vendors (or suppliers) to assist in managing known vulnerabilities and to deliver more secure systems. When building cybersecurity into the procurement process, owners and operators should realize that system environments, technologies, and risks may vary. As such, the cybersecurity language for the procurement of a particular product or service should match the cybersecurity policies of the environment into which the product/service will be integrated or applied. In addition, vendor or contractor access to the system should be controlled (e.g., manually initiated) to ensure system security.

An owner or operator may have decreased visibility into, understanding of, or control over how an acquired technology is developed, integrated, and deployed, as well as the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of the products and services. To understand vendor security threats and vulnerabilities, an owner or operator can implement supply chain risk management. Part of an effective supply chain risk management program is conducting risk assessments and analysis along the supply chain and establishing a vendor security program. Any vendor's security systems and procedures should be designed and implemented in accordance with standards and accepted industry practices.

Effective vendor security programs incorporate a standardized process to address supply chain risk with respect to control systems and IT systems, and to inform the acquisition process of threats, risks, and required security controls. NIST SP 800-53 covers system and services acquisition—including supply chain security controls—in more detail. Vendor security programs should, at a minimum, include the following elements:

- **Vendor Assessment:** This is designed to gather information regarding a current or prospective vendor's cybersecurity and information privacy, confidentiality, and practices. The assessment can be designed as a questionnaire with summary of purpose, definitions (to ensure consistency and minimize confusion), general contact and vendor information, and the security controls for assessment.
- **Contractual Vendor Provisions:** Whenever explicit agreements are feasible and practical (e.g., through contracts or service-level agreements), organizations should develop agreements that require the use of the security controls consistent with the guidance in this document. One example is to include provisions for the protection of stored information into agreements with system integrators, suppliers, and external service providers.
- **Life Cycle Management Policy:** A well-defined system life cycle management policy provides the foundation for the successful development, implementation, and operation of organizational information systems. Applying the required security controls within the system life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. In developing a life cycle management policy, owners and operators may consider referencing the DHS Build Security In initiative—a collaborative effort that provides best practices, knowledge, tools, and resources to build security into software in every phase of its development.
- **In-house and Third-Party Testing:** Infrastructure vulnerability assessments can be accomplished through in-house services or third-party testing. Owners and operators are encouraged to fully vet potential in-house or third-party testing services prior to hiring. One example of such testing services is the DHS-offered National Cybersecurity Assessment and Technical Services (NCATS), which provides a third-party perspective on the current cybersecurity posture of the infrastructure and systems. Services like NCATS provide reliable, objective testing to uncover vulnerabilities. This is particularly important as some organizations do not allow products/systems to be connected to infrastructure unless that infrastructure undergoes objective vulnerability testing.

For additional information, refer to the applicable security controls in NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, *Cybersecurity Procurement Language for Energy Delivery Systems*, and the vendor questionnaires in Appendix E and F.

Cybersecurity Awareness

To advance cybersecurity risk management, organizations can leverage internal risk assessment results to inform and improve their policies, procedures, and security measures. Organizations should also ensure their personnel understand the organization's cybersecurity policies, procedures, and security measures; are up-to-date on cybersecurity best practices; and maintain knowledge commensurate with the cyber threat. This occurs through the development of an internal training program, which can be simple (e.g., cybersecurity basics for all personnel) or complex (e.g., knowing common attack vectors and how to prevent/mitigate attacks). Effective training is ongoing and identifies current best practices and standards. To supplement cybersecurity awareness programs, organizations can leverage external training and information (e.g., alerts, threat information, analysis, best practices) obtained from Federal government departments and agencies, information sharing and analysis centers, and other sources in pursuit of cybersecurity risk management. This may also include participating in sector programs that facilitate cybersecurity knowledge transfer.

Organizations can use the following mechanisms to build personnel cybersecurity awareness.

- **ICS-CERT** operates within the DHS National Cybersecurity and Communications Integration Center (NCCIC) and collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. ICS-CERT also hosts a variety of cybersecurity training opportunities.
- **United States Computer Emergency Readiness Team (US-CERT)** operates within the NCCIC, alongside ICS-CERT. US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities.

- **Cyber Information Sharing and Collaboration Program (CISCP)** is a DHS program for public-private information sharing. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities within a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses.
- **Multi-State Information Sharing and Analysis Center (MS-ISAC)** provides workforce development resources, real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

For additional information, refer to the *Dams Sector Security Guidelines*, *NIST Cybersecurity Framework Implementation Guide*, and the NCCIC Website.

Information Security Classifications

Typically, information is stored in a protected manner based on the sensitivity and confidentiality of the information. The owner of the information is responsible for appropriately classifying, labeling, handling, and destroying information. In identifying, classifying, and distributing sensitive information, owners and operators generally follow their internal company policies and procedures and comply with all applicable regulatory requirements and laws. Once information assets are identified and effectively classified, an organizational information security policy can be established to protect the various information assets.

To ensure consistent classification and subsequent protection of information, procedures can be developed to mark, store, and transmit information. The following represents private sector classification levels in handling and processing requests for information, and is not an exhaustive listing of classification levels or designations across the sector.

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

Using, processing, storing, reproducing, transmitting, and destroying classified United States Government information must be completed under the appropriate information classification and security regime and must be consistent with the appropriate laws, executive orders, directives, regulations, and authorized agency controls. Federal Government agencies should follow Federal information classification guidelines. State and local facilities should follow their respective guidelines and apply Federal information classification guidelines when handling information created or received by an agency of the Federal Government.

For additional information, refer to the *Dams Sector Security Guidelines* and the NERC *Security Guideline for the Electricity Sector: Protecting Sensitive Information*.

Risk Management Guidelines and Frameworks

- **DOE *Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*** provides the Dams Sector with examples of effective and efficient risk management processes.
- **NERC *Critical Infrastructure Protection Reliability Standards*** define the reliability requirements for planning and operating the North American bulk power system and were developed using a results-based approach that focuses on performance, risk management, and entity capabilities. These standards include CIP Standards 001 through 009 that address the security of cyber assets essential to the reliable operation of the electric grid.
- **NIST *Framework for Improving Critical Infrastructure Cybersecurity*** provides a common language that organizations can use to assess and manage cybersecurity risk. It recommends risk management processes that enable organizations to inform and prioritize decisions regarding cybersecurity based on business needs without additional regulatory requirements. It enables organizations—regardless of sector, size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. Each sector and individual organization can tailor the Framework to address its cybersecurity objectives. NIST developed additional guidance to assist sector-specific critical infrastructure owners and operators in understanding and using the Framework:
  - **Dams Sector Cybersecurity Framework Implementation Guidance** seeks to help Dams Sector owners and operators understand and use the Framework. The guidance presents background information on the Framework, benefits Dams Sector organizations can realize from using the Framework, a mapping of existing Dams Sector tools and approaches that can facilitate Framework implementation, and Framework Implementation Steps.
  - **Energy Sector Cybersecurity Framework Implementation Guidance** seeks to help Energy Sector owners and operators understand and use the Framework. The guidance is tailored to the sector's risk environment and existing cybersecurity and risk management tools and processes that organizations can use to implement the Framework.

4. Response and Recovery

Dams are vital to the operation of a wide variety of infrastructure that meet the Nation's essential needs, including potable water, navigation and transportation, energy production and distribution, and a host of commercial support functions. The loss of a single dam could disrupt a community or region for months or even years. The consequence from such an event can be substantially reduced not only through proper planning and resource readiness, but also rapid response and recovery. Response and recovery planning are critical elements to a cybersecurity program. These may include procedures for incident response, continuity of operations, and disaster recovery. This guidance provides a comprehensive approach with recommended strategies to plan for a cybersecurity incident response and recovery. The approach includes the following elements:

- Understand appropriate response activities to implement as part of preparedness or regarding a detected cybersecurity incident
- Develop and implement appropriate activities to maintain resilience and restore disrupted capabilities or services (due to a cybersecurity event)

Incident Response

Incident response is an important element of a control system cybersecurity program. Incident response capabilities are necessary for detecting incidents rapidly, minimizing disruptions of system operations, mitigating weaknesses that may have been exploited, and restoring services. Effective incident response is a complex undertaking; and, therefore, establishing a successful incident response capability requires substantial planning and resources.

The NIST *Computer Incident Handling Guide* (NIST SP 800-61) provides guidelines for incident response, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. General guidelines for incident response include:

- Develop a formal incident response capability, such as an incident response policy or plan, or incorporate incident response procedures into existing risk management plans. Plan or procedures include:
  - Procedures for performing incident handling and reporting
  - Incident response team structure, staffing model, services, and training
  - Guidelines and methods for communicating with outside parties regarding incidents
- Focus incident response on being prepared to handle incidents that use common attack vectors, such as:
  - External or removable media (e.g., flash drive, CD, or a peripheral device)
  - Websites or web-based applications
  - E-mail messages or attachments
  - Violation of an organization's acceptable usage policies by an authorized user
  - Loss or theft of a computing device or media used by the organization (e.g., laptop, smartphone, or computer tablet)
- Emphasize the importance of incident detection and analysis throughout the organization, including establishing logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.

- Develop written guidelines for prioritizing incidents to identify situations that are of greater severity and demand immediate attention. Incidents should be prioritized based on relevant factors, such as the functional impact of the incident, the information impact of the incident, and the recoverability from the incident.
- Leverage a lessons-learned process to adapt and derive value from incidents, including organizing meetings to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices.

Continuity of Operations

Continuity of operations (COOP), or business continuity, focuses on restoring an organization's mission-essential functions (e.g., electric power for necessary unit auxiliaries, programmable logic controllers for control systems, and personal computers for control systems actions) after a major incident. Depending on the severity of an incident, these functions may be performed at an alternate site for an extended period of time (i.e., 30 days or more) before returning to normal operations. COOP plans are employed by organizations to reach effective COOP in the face of major disruptions.

Standard elements of a COOP plan are listed in the NIST *Contingency Planning Guide for Federal Information Systems* (SP 800-34) and may be referenced for developing COOP plan provisions for control systems. These standard elements include:

- Program plans and procedures
- Continuity communications
- Risk management
- Vital records management
- Budgeting and acquisition of resources
- Human capital
- Essential functions
- Test, training, and exercise
- Order of succession
- Devolution
- Delegation of authority
- Reconstitution
- Continuity facilities

Disaster Recovery

If the disruptions from an incident are extensive, disaster recovery actions are employed. A disaster recovery plan (DRP) applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. It is supported by an incident response team, contains specific procedures to implement, and is tested regularly. The DRP typically only addresses information system disruptions that require relocation, and may be supported by other incident response plans to address recovery of impacted individual systems once the alternate facility has been established. See the NIST *Contingency Planning Guide for Federal Information Systems* (SP 800-34) for further information.

Appendix A. Acronyms

C2M2	Cybersecurity Capability Maturity Model
CERT	Computer Emergency Response Teams
CIP	Critical Infrastructure Protection
CISCP	Cyber Information Sharing and Collaboration Program
COOP	Continuity of operations
CRA	Cybersecurity Risk Assessment
CRR	Cyber Resilience Review
CSET	Cyber Security Evaluation Tool
CTS	Consequence-Based Top Screen
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DRP	Disaster recovery plan
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FTP	File transfer protocol
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
HVAC	Heating, ventilation, and air conditioning
IaaS	Infratructure as a Service
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IP	Internet Protocol
IT	Information technology
MS-ISAC	Multi-State Information Sharing and Analysis Center

NCATS	National Cybersecurity Assessment and Technical Services
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
NIST	National Institute of Science and Technology
NTAS	National Terrorism Advisory System
OT	Operational technology
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
RMP	Risk Management Process
SaaS	Software as a Service
SCADA	Supervisory control and data acquisition
SP	NIST Special Publication
SSI	Sensitive security information
SSL	Secure Sockets Layer
SVA	Security vulnerability assessment
TLS	Transport Layer Security
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual private network

Appendix B. Types of Cyber Systems

The following chart of cyber system types provides examples of each type, consistent with the definition of cyber systems included in the *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*.

Cyber System Type	Description	Examples
Business Systems	Cyber systems used to manage or support common business processes and operations.	• Enterprise Resource Planning • E-commerce • E-mail • Research and development systems • Underlying security control systems, including internal and external (boundary) systems • Digital assets that provide security (e.g., firewalls)
Control Systems	Cyber systems used to monitor and control sensitive processes and physical functions within many infrastructures and industries. Control systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators).	• Supervisory Control and Data Acquisition Systems • Process Control Systems (e.g., continuous automatic regulation of facility operations or processes) • Distributed Control Systems (e.g., centralized supervisory control of a group of localized process control systems) • Security Control Systems (e.g., control of cyber or physical security access, surveillance, and monitoring)
Access Control and Specialty Systems	Cyber systems allowing only authorized personnel and visitors physical access to defined areas of a facility and systems used for alert and warning purposes, as well as other sector-specific cyber systems that are not accounted for in business and control systems. Access control systems provide monitoring and control of personnel passing throughout a facility by various means, including electronic card readers, biometrics, and radio frequency identification. Warning systems pass critical information that triggers protection and response actions for formal organizations and individual citizens. Examples include local phone-based hazard alerting systems used by some local governments, the Emergency Alert System established by the Federal Communications Commission, and its National Oceanic and Atmospheric Administration Weather Radio, which is an all-hazards alerting system provided by the U.S. Department of Commerce. Specialty systems encompass any additional sector-specific cyber systems that may be used to support the operation or delivery of a sector's critical functions.	• Access Control Systems • Warning Systems • Environmental Monitoring Systems (e.g., localized weather, water/air quality, and heating, ventilation, and air conditioning monitoring) • Emergency Preparedness Systems

Appendix C. TSA Baseline and Enhanced Security Measures

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

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

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

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

Appendix D. Cyber and Physical Security Measures for Dams Sector Owner and Operators

The following charts of security measures are amended from *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (NIST 800-53).

General Cybersecurity Measures

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative	Owner/operator designates one or more individuals to manage cybersecurity who can demonstrate proficiency in developing cybersecurity policies and procedures and ensuring compliance with all applicable industry and governmental cybersecurity requirements through a combination of training, education, and/or experience.	AU-4
Administrative	Owner/operator monitors and conducts a periodic review, at least on an annual basis, of network connections, including remote and third-party connections.	
Administrative	Owner/operator evaluates and assesses the role of wireless networking for risk before implementation.	IA-7
Administrative	Owner/operator reviews and reassesses all cybersecurity procedures annually. The owner/operator updates procedures as necessary.	
Administrative	Owner/operator reviews and reassesses cyber asset criticality periodically, at least on an annual basis.	PM-1

Information Security Coordination and Responsibilities

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative	Owner/operator develops an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks.	AU-3
Administrative	Owner/operator defines information and cybersecurity roles, responsibilities, and lines of communication among the operations, IT, and business groups, as well as with outsourcers, partners, and third-party contractors.	IA-3
Administrative	Owner/operator establishes and documents standards for cybersecurity controls to be used when evaluating systems and services for acquisition. Encourage vendors to follow software development standards for trustworthy software throughout the development lifecycle.	SA-1, SA-2, SA-3

System Lifecycle

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative	Owner/operator incorporates security into cyber system design and operation, whether designing a new system or modifying an existing system. Secure design and operation of the supervisory control and data acquisition (SCADA) system architecture is critical to ensure a sustainable and reliable system. Mitigate any security deficiencies found in control system hardware and software.	SA-1, SA-2, SA-3
Administrative	Owner/operator establishes and documents policies and procedures for assessing and maintaining system status and configuration information, for tracking changes made to the control systems network, and for patching and upgrading operating systems and applications.	SA-1, SA-2, SA-3
Administrative	Owner/operator integrates cybersecurity into the system lifecycle (i.e., design, procurement, installation, operation, and disposal). Owner/operator establishes security requirements for all systems and networks before putting them into operation and for all operational systems and networks throughout their lifecycle.	SA-1, SA-2, SA-3
Administrative	Owner/operator documents a business need for all networks, systems, applications, services, and external connections.	PM-1, PM-2
Logical	Owner/operator identifies hardware, software, information, and services and disables all unnecessary elements where technically feasible. Owner/operator also identifies and evaluates potential vulnerabilities and implements appropriate compensating security controls.	
Administrative	Owner/operator performs an asset inventory of all critical IT systems and develops a cohesive set of network/system architecture diagrams or other documentation including nodes, interfaces, and information flows.	PM-1

System Response and Recovery

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative	Owner/operator plans and prepares for the restoration and recovery of control systems in a timely fashion as specified in the owner or operator's recovery procedures.	AU-7, SA-5
Logical	Owner/operator employs cybersecurity measures at alternate facility operations and within primary facility recovery/reconstitution phases that are consistent with those in place within the original operational functions.	AU-5, AU-6, AU-7, PE-1 to PE-9

Intrusion Detection and Response

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative and Logical	Owner/operator establishes policies and procedures for cyber intrusion monitoring, detection, incident handling, and reporting. Owner/Operator implements these controls as necessary.	SC-3
Logical	Owner/operator implements cybersecurity controls to prevent malicious code from exploiting cyber systems and applies appropriate software security patches and updates to systems as soon as possible given critical operational and testing requirements.	SC-10
Logical	Owner/operator monitors networks for unauthorized access or the introduction of malicious code in near-real time with immediate alerts, logs cybersecurity events, reviews the logs daily, and responds to alerts in a timely manner. Network monitoring may occur onsite or offsite. Where logging of cybersecurity events on their networks is not technically feasible (e.g., logging degrades system performance beyond acceptable operational limits), implement appropriate compensating security controls (e.g., monitoring at the network boundary).	SC-4, SC-5, SC-6
Administrative	Owner/operator reports significant cyber incidents to senior management and to regulatory authorities as required. Use of ICS-CERT for incident response is highly recommended.	AT-3, IR-1, IR-2, IR-3

Training

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative	Owner/operator provides training in information security awareness to all users of control systems before permitting access to the control systems and on an annual basis or as necessitated by changes in the control system. Individuals with significant control systems security roles should have training specific to their roles.	AT-1, AT-2

Access Control and Functional Segregation

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative	Owner/operator establishes and documents a business requirement for every external connection to/from its cyber systems, and external connections have controls that permit access only to authorized and authenticated users.	SC-12
Administrative and Logical	Owner/operator identifies network boundaries, and segregates and protects the control systems network from the business network and the Internet with firewalls and other protections. This applies both to wired and wireless networks.	SC-3
Administrative	Owner/operator uses control systems hosts and workstations only for approved control system activities.	IA-11
Logical	Owner/operator establishes and enforces access control policies for local and remote users, guests, and customers. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections to control networks.	SC-12
Logical	Owner/operator practices the concept of least privilege and implements control to enforce this concept, where applicable.	IA-10
Logical	Owner/operator documents and enforces authentication methods (including password structures) for all administrative and user accounts. Additionally, owner/operator changes all default passwords and ensures that default passwords for new software, hardware, etc., are changed upon installation. In instances where changing default passwords is not technically feasible (e.g., a control system with a hard-coded password), the owner/operator implements appropriate compensating security controls (e.g., physical controls).	IA-1, SI-3, SI-5
Logical	Owner/operator defines allowable remote access (e.g., Internet, virtual private network (VPN), modems) and rules of behavior. Those rules describe user responsibilities and expected behavior with regard to information system usage, to include remote access activities (e.g., appropriate Websites, conduct of personal business).	SC-12
Logical and Physical	Owner/operator restricts physical and logical access to control systems and control networks with an appropriate combination of locked facilities, passwords, communications gateways, access control lists, authenticators, and separation of duties, invocation of least privilege, and/or other mechanisms and practices.	

Personnel Security

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Physical	Owner/operator reviews and establishes security requirements for positions that permit physical access to critical cyber systems. Owner/operator implements role-based physical security to restrict access to cyber system assets and information storage media.	MP-1
Logical	Owner/operator establishes and enforces unique accounts for each individual user and administrator. Owner/operator establishes security requirements for certain types of accounts (e.g., administrative access to the system) and prohibits the sharing of accounts. In instances where users function as a group (e.g., control system operators) and user identification and authentication is role based, implement appropriate compensating security controls (e.g., physical controls).	IA-1
Administrative and Logical	IT management, systems administration, and IT security duties should not be performed by the same individual. In instances where this is not feasible, implement appropriate compensating security controls (e.g., administrative controls, such as review and oversight).	CM-3, CM-4
Administrative	Owner/operator maintains access control lists and ensures that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated expeditiously for personnel leaving under adverse action and when users no longer require access (e.g., when personnel leave the company, complete a transfer into a new role, or their responsibilities change).	
Administrative	Owner/operator ensures that service providers and other third parties with responsibilities for cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel surety requirements for the owner or operator's employees.	

Vulnerability Assessment

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative and Logical	Owner/operator conducts periodic vulnerability assessments of the control system security, including appropriate testing in a non-production environment at intervals of no more than every 24 months or on a schedule dictated by regulatory authority.	

Audit

Security Control Type	Security Measure Description	Framework Core Functions Mapping
Administrative	Owner/operator conducts regular audits that measure compliance with cybersecurity policies, plans, and procedures and reports audit results to senior management.	AU-1

Appendix E. Supply Chain Cybersecurity Risk Management Intake Questionnaire

The Supply Chain Cybersecurity Risk Management Intake Questionnaire is designed for an owner or operator to complete for their respective vendors in order to classify the vendor and determine an initial level of risk associated with engaging in business relations with the vendor.

General Information

Contact Information

Name of Company Employee Completing Form:	
Company Employee Job Title:	
Company Employee E-Mail Address:	
Date Completed:	

Fill out the following table with the vendor's information:

Vendor Name:	
Vendor Address(es) (including offshore locations):	
Vendor Business Contact Name, E-Mail Address, and Phone Number:	
Vendor IT Contact Name, E-Mail Address, and Phone Number:	
Vendor IT Security Contact Name, E-Mail Address, and Phone Number:	

Seek Director approval prior to submitting this form:

Director Name and Line of Business:	
Director Signature:	
Date Completed:	

Questionnaire

No.	Question	Response
1.	Describe in detail the product or service being provided by the vendor to the company.	
2.	Describe in detail the type of data elements the company will be sharing with the vendor (e.g., customer or employee name, addresses, customer energy usage data, social security numbers).	
3.	How many records will be shared with the vendor?	❑ < 500 ❑ 500 – 50,000 ❑ > 50,000
4.	What is the classification of the data that is being shared with the vendor?	❑ Public ❑ Internal ❑ Confidential ❑ Restricted ❑ Privileged
5.	Is the vendor's service to the Company part of any Public Utilities Commission mandate?	❑ Yes ❑ No
6.	Will the vendor be receiving customer and/or employee data from a source other than the company? If yes, is this collected on the company's behalf?	❑ Yes ❑ No
7.	Describe in detail the type of network connectivity the vendor will require to the company network (e.g., Virtual Private Network, Citrix, business-to-business, leased line).	
8.	Will the vendor provide or modify any software or firmware, hardware digital components, or equipment that may interact with or control a company system (e.g., IT, operational technology, critical assets)?	❑ Yes ❑ No
9.	Will the device or equipment communicate with other digital devices or equipment, or be part of a network?	❑ Yes ❑ No
10.	Will the vendor install a software agent on company systems that will send information back to the vendor?	❑ Yes ❑ No
11.	What type of cloud service will the vendor be hosting on behalf of the company?	❑ Platform as a Service (PaaS) ❑ Infrastructure as a Service (IaaS) ❑ Software as a Service (SaaS) ❑ Other ❑ Not Applicable
12.	Will the vendor send e-mail or make phone calls on behalf of the company?	❑ Sending e-mail ❑ Making Phone Calls ❑ Both
13.	Will the vendor subcontract part of the service to one of its third parties?	❑ Yes ❑ No

Appendix F. Supplier Assessment Questionnaire – Data Privacy and Security

The Supplier Assessment Questionnaire – Data Privacy and Security gathers information regarding the prospective supplier's personal information privacy, confidentiality, and security practices. The Project Manager is responsible for completing Section 1.A., and the supplier is responsible for completing Sections 1.B. and 2.

1. General Information

A. Completed by Project Manager

Contact name, phone number, and e-mail address	
Proposed project start date	
Proposed end date, if known	
Describe the authorized functions or activities that supplier will perform for or on behalf of the company	

B. Completed by Supplier

Supplier name	
Supplier contact name, phone number, and e-mail	
Contact information for supplier's employee or employees responsible for privacy and information security	
Date supplier completed this questionnaire	
Will supplier access, collect, use, store, disclose, modify, dispose of or otherwise process personal data in connection with the performance of authorized functions or activities for or on behalf of the company?	❑ Yes ❑ No If yes, complete Part 2 of this questionnaire.

2. Privacy and Information Security Practices (Completed by Supplier)

No.	Question	Response
1.	Whose personal data will supplier access in connection with the performance of authorized functions or activities for or on behalf of?	Check all that apply: ❑ Personnel (e.g., applicants, current or former employees, consultants) ❑ Customers ❑ Supplier personnel ❑ Others (please specify): _____
2.	What actions will supplier perform with respect to personal data?	Check all that apply: ❑ Collect personal data from customers ❑ Collect personal data from personnel ❑ Access personal data maintained by suppliers or other third parties ❑ Store personal data ❑ Disclose personal data to third parties ❑ Dispose of personal data ❑ Others (please specify): _____
3.	Describe the sources from which supplier will obtain personal data.	Check all that apply: ❑ Customers ❑ Employees ❑ Suppliers (please specify): _____ ❑ Other (please specify): _____
4.	What types of personal data will supplier access?	Check all that apply: ❑ Protected health information (PHI) ❑ Personally identifiable information (PII) ❑ Social Security Number ❑ Driver's license number ❑ Government-issued identification number ❑ Credit or debit card number ❑ Financial account number or other information that permits access to an individual's financial account ❑ Any individually identifiable information received from a financial institution, such as a bank or mutual fund company ❑ Consumer report information provided by Equifax, Experian, TransUnion, Social Intelligence, or another reporting agency ❑ Individually identifiable biometric data (e.g., retina/iris scan or fingerprint) ❑ Employer-issued system password ❑ First name and last name, with any one of the following: ❑ Date of birth ❑ Mother's maiden name ❑ Digitized or other electronic signature ❑ DNA Profile ❑ Private Data on Individuals ❑ Name ❑ Address ❑ E-mail address ❑ Social media identifier ❑ Other online persistent identifier (e.g., IP address) ❑ Telephone number ❑ Fax number ❑ Postal address

No.	Question	Response
	What types of personal data will supplier access? (continued)	❑ Customer information: ❑ Account number or debtor number ❑ "My Account" user name and password ❑ Type or classification of service ❑ Energy usage ❑ Expected patterns of energy use ❑ Types of facilities used in providing utility service ❑ Current charges ❑ Billing records ❑ Finances ❑ Occupation ❑ General reputation ❑ Credit ❑ Health (e.g., medical devices at a customer's home or customer's relevant health condition) ❑ Other personal characteristics ❑ Employee information: ❑ Employment history and health information ❑ Compensation information (including salary, incentive, and pension) ❑ Performance ratings ❑ Disciplinary records and grievance files ❑ Security application ❑ Protected class status (e.g., age, ethnic group, disability) ❑ Nuclear access records ❑ Criminal history ❑ Other Personal Data that is not PHI or PII (specify) _____
5.	Will supplier store, process, handle, or transmit credit, debit, or other payment card data in connection with the performance of authorized functions or activities for or on behalf of the company?	❑ Yes ❑ No If yes, is the supplier fully compliant with the Payment Card Industry Data Security Standard ("PCI DSS")? ❑ Yes ❑ No If no, please describe any non-compliance. Specify whether supplier performed a PCI DSS self-assessment or was certified as PCI DSS compliant by an assessor. Please specify the assessor. What is the date of the certification? Please provide copies of documents verifying compliance with PCI DSS.
6.	Will supplier access, collect, store, use, disclose, or otherwise process personal data in aggregated or de-identified format?	❑ Yes ❑ No If yes, describe how personal data will be aggregated or anonymized, and how and for what purposes the supplier will process the data.

No.	Question	Response
7.	Describe the purposes for which supplier will access personal data.	Check all that apply: ❑ Customer service and support ❑ Managing and maintaining customer information ❑ Invoicing and billing ❑ Payment processing ❑ Verification/authentication of personal data ❑ Information technology support ❑ Human resources support ❑ Recruiting ❑ Investor relations ❑ Marketing ❑ Data analytics, including market research ❑ Disposal of information (e.g., shredding, burning, pulverizing) ❑ Compliance (including fraud prevention) ❑ Other (please specify): _____
8.	Specify the media in which supplier will obtain or access personal data.	Check all that apply: ❑ Electronic (e.g., downloaded files, CDs, DVDs) ❑ Hard copy ❑ Other (please specify): _____
9.	Describe the means by which personal data will be transferred between supplier and the company.	Check all that apply: ❑ Secure File Transfer Protocol (FTP) ❑ Secure Sockets Layer (SSL) ❑ Transport Layer Security (TLS) ❑ VPN ❑ Website(s) ❑ E-mail ❑ Telephone ❑ Fax ❑ Secure mail delivery service (e.g., FedEx, UPS, DHL, interoffice pouch) ❑ Other (please specify): _____
10.	Specify individuals and entities that will have access to personal data.	Check all that apply: ❑ Supplier's employees ❑ Supplier's subcontractors or consultants (please specify): _____ ❑ Supplier's marketing partners (please specify): _____ ❑ Others (please specify): _____
11.	Will supplier make personal data available or accessible to any person or entity located outside the United States?	❑ Yes ❑ No If yes, describe (i) the geographical location to which the information may be transferred or from which the information may be accessible, and (ii) the purpose of the transfer of, or access to, the information. (i)_____ (ii)_____

No.	Question	Response
12.	Describe the means by which supplier will transmit personal data to third parties.	Check all that apply: ❑ Secure FTP ❑ VPN ❑ SSL ❑ TLS ❑ Website(s) ❑ E-mail ❑ Telephone ❑ Fax ❑ Secure mail delivery service (e.g., FedEx, UPS, DHL, interoffice pouch) ❑ Other (please specify): _____
13.	Describe how service provider will store electronic personal data.	Check all that apply: ❑ Supplier's servers ❑ Third-party servers ❑ E-mail folders ❑ Supplier's computers ❑ Portable electronic devices (e.g., CDs, DVDs, tapes, flash drives, etc.) ❑ Other (please specify): _____
14.	Describe the physical location where supplier will store hard-copy personal data.	Check all that apply: ❑ Controlled-access facilities ❑ Locked file cabinets ❑ Other (please specify): _____
15.	Describe supplier's back-up procedures for electronic personal data.	By what method is the information backed up (e.g., tape, disk)? _____ How often is the information backed up? _____ Where are back-ups maintained (e.g., offline, offsite)? _____ How long are back-ups maintained? _____ How often are back-ups disposed of? _____ How are back-ups disposed of (e.g., recycled, physically destroyed)? _____ How often are restore tests performed? _____
16.	Does the supplier maintain a comprehensive, written information security program that includes administrative, technical, and physical safeguards designed to: • Ensure the privacy, confidentiality, security, integrity, and availability of personal data? • Protect against any anticipated threats or hazards to the security and integrity of personal data? • Protect against any information security incident that may affect personal data?	❑ Yes ❑ No If yes, please provide a copy.

No.	Question	Response
17.	Does supplier regularly test and monitor key administrative, technical, and physical controls, systems, and procedures that safeguard personal data?	❑ Yes ❑ No If yes, how often is testing performed? _____ Please provide documentation of the testing, if available.
18.	Does supplier conduct periodic privacy and information security risk assessments to identify and assess the risks to personal data in supplier's operations?	❑ Yes ❑ No If yes, how often are risk assessments performed? ❑ _____ Please provide a copy of the most recent risk assessment.
19.	Does supplier periodically review how it collects, uses, maintains, discloses, and disposes of personal data?	❑ Yes ❑ No
20.	Does supplier periodically inventory information systems and assets, including mobile devices that contain personal data?	❑ Yes ❑ No
21.	Does supplier maintain procedures requiring secure disposal of electronic and hard-copy records containing personal data after it is no longer needed to comply with business purposes or legal obligations?	❑ Yes ❑ No If yes, does supplier maintain a policy to remove personal data from electronic media before disposal or re-use of the media? ❑ Yes ❑ No Does supplier maintain technical measures to securely dispose of personal data stored on servers, desktops, mobile storage devices, and other electronic media so that the information cannot practicably be read or reconstructed? ❑ Yes ❑ No Describe how supplier disposes of disk drives and other electronic hardware that contains personal data, as well as hard-copy media: ❑ Burning ❑ Pulverizing ❑ Shredding ❑ Using a qualified supplier (please specify the supplier): _____ ❑ Other methods (please specify): _____
22.	Does supplier maintain a privacy and security awareness and training program for personnel and third parties who access personal data?	❑ Yes ❑ No If yes, provide a copy of training materials.
23.	Does supplier have a policy to limit access to personal data to personnel and third parties that have a documented need to access the information to fulfill their business functions?	❑ Yes ❑ No
24.	Does supplier regularly review access permissions to personal data to ensure that only need-to-know personnel and third parties have access?	❑ Yes ❑ No
25.	Does supplier have a procedure for promptly preventing terminated personnel and third parties from accessing personal data?	❑ Yes ❑ No

No.	Question	Response
26.	Does supplier conduct background checks of personnel or third parties who have access to personal data?	❑ Yes ❑ No If yes, check all that apply: ❑ Criminal background checks (e.g., national federal criminal database check, country of residence criminal conviction search, terrorist watch lists, etc.) ❑ Address verification ❑ Education verification ❑ Credit and financial history search ❑ Employment history verification ❑ Personal references verification ❑ Drug screening ❑ Other (please specify): _____
27.	Does supplier practice separation of duties to reduce opportunities for unauthorized or unintentional modification or misuse of personal data?	❑ Yes ❑ No
28.	Does supplier have a policy to discipline employees who fail to comply with personal data privacy or security policies and procedures?	❑ Yes ❑ No
29.	Will supplier use subcontractors to provide services that may involve access to personal data?	❑ Yes ❑ No If yes, please provide: Service Type: _____ Subcontractor Name: _____ Countries where the service will be performed: _____ Has supplier audited or reviewed the subcontractors' privacy and information security safeguards? ❑ Yes ❑ No Has the audit or review resulted in a finding that the subcontractors provide an adequate level of privacy and information security safeguards? ❑ Yes ❑ No
30.	Does supplier contractually require subcontractors to maintain adequate safeguards for personal data that are at least equivalent to the safeguards that the organization must implement pursuant to contractual or legal requirements?	❑ Yes ❑ No
31.	Does supplier maintain a comprehensive information security incident response process?	❑ Yes ❑ No If yes, provide a copy of the relevant procedure.
32.	Does supplier have an information security incident response team?	❑ Yes ❑ No

No.	Question	Response
33.	Has supplier experienced an information security incident in the preceding three years?	❑ Yes ❑ No If yes, please describe the incidents. _____
34.	Does supplier have insurance coverage for information security incidents?	❑ Yes ❑ No If yes, provide a copy of the policy.
35.	Does supplier maintain contingency and disaster recovery plans designed to create and maintain copies of covered information, restore any loss of covered information, and continue critical business processes involving covered information in emergency mode, and periodically test and update the plans.	❑ Yes ❑ No
36.	Does supplier maintain technical controls to (i) allow only authorized personnel (including only active users) to access personal data and (ii) authenticate authorized users?	❑ Yes ❑ No
37.	Does supplier block user access after multiple unsuccessful attempts to gain access to personal data or relevant information systems and terminate user access after a predetermined period of inactivity?	❑ Yes ❑ No
38.	Does supplier terminate electronic sessions after a predetermined time of inactivity or implement automatic logoff, including for workstations?	❑ Yes ❑ No
39.	Does supplier employ multi-factor user authentication?	❑ Yes ❑ No If yes, describe which authentication technologies are used and the circumstances in which they are used. _____
40.	Does supplier require personnel to (i) use unique passwords (that are not vendor-supplied default passwords) for access to personal data and (ii) safeguard the passwords?	❑ Yes ❑ No
41.	Does supplier maintain secure control over user identification, passwords, and other authentication identifiers?	❑ Yes ❑ No If yes, describe the controls. _____
42.	Does supplier require personnel to (i) change passwords at regular intervals or based on the number of access attempts and whenever there is any indication of possible system or password compromise and (ii) avoid reusing or recycling old passwords?	❑ Yes ❑ No
43.	Does supplier monitor log-in attempts and report discrepancies?	❑ Yes ❑ No
44.	Does supplier maintain up-to-date firewalls between the organization's information systems, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks that are not necessary for processing personal data?	❑ Yes ❑ No
45.	Does supplier utilize software that detects, prevents, removes, and remedies malicious code designed to perform an unauthorized function on, or permit unauthorized access to, any information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs.	❑ Yes ❑ No

No.	Question	Response
46.	Does supplier regularly update malicious code detection software, including virus signatures, definitions, and patches?	❑ Yes ❑ No If no, describe how often these processes and updates are run. If yes, how often do you update the software?
47.	Does supplier instruct its employees and contractors to limit the storage of personal data on mobile storage devices to the minimum required for business purposes?	❑ Yes ❑ No
48.	Does supplier allow personnel to use personally owned devices on the supplier's network?	❑ Yes ❑ No If yes, describe the security measures that apply. _____
49.	Does supplier ensure strong encryption of personal data?	❑ Yes ❑ No If yes, describe when encryption is required: ❑ Personal data stored on laptops or mobile devices ❑ Personal data stored outside of the organization's physical controls ❑ Personal data transmitted across any public network (such as the Internet) or wirelessly ❑ Personal data transmitted outside of the organization's information systems ❑ Other circumstances (please describe): _____
50.	Does supplier maintain technical measures to guard against unauthorized access to electronically transmitted personal data?	❑ Yes ❑ No
51.	Does supplier maintain measures to secure wireless access to information systems?	❑ Yes ❑ No
52.	Does supplier maintain measures to secure remote access to information systems?	❑ Yes ❑ No
53.	Does supplier's change management process include controls to ensure that information system modifications are consistent with the supplier's information security program?	❑ Yes ❑ No
54.	Does supplier maintain electronic mechanisms to corroborate that covered data has not been altered or destroyed without authorization?	❑ Yes ❑ No
55.	Does supplier maintain hardware and software mechanisms that record and examine activity in information system or monitor and review records of system activity, including for purpose of detecting unauthorized access to personal data?	❑ Yes ❑ No If yes, describe the mechanisms. _____

No.	Question	Response
56.	Does supplier maintain physical safeguards for data systems (including workstations) that contain or facilitate access to personal data and the facilities in which the equipment is located?	❑ Yes ❑ No If yes, check all security measures that apply to the storage of any media (e.g., hard copies, desktops, laptops, servers, etc.) that may contain personal data: ❑ Escort-only facility entry for visitors ❑ Locked rooms ❑ Locked cabinets ❑ Badge-reading systems ❑ Security key fobs ❑ Video surveillance systems ❑ Alarms ❑ Security guards ❑ Other measures (describe): _____
57.	Does supplier maintain controls governing the physical security of the storage, access, transportation, and destruction of records or media containing personal data outside of the organization's business premises?	❑ Yes ❑ No If yes, describe the controls. _____
58.	Does supplier maintain physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or manmade disaster?	❑ Yes ❑ No If yes, describe the controls. _____
59.	Does supplier maintain procedures that govern the receipt, removal, and movement of hardware and media containing personal data?	❑ Yes ❑ No
60.	Does supplier document repairs and modifications to its computer networks?	❑ Yes ❑ No
61.	Does supplier store back-up or archival media, workstations, or network equipment that may be used to access personal data in physically secure areas?	❑ Yes ❑ No If yes, describe how the hardware is stored. _____
62.	Does supplier adhere to any technology security standards (e.g., International Organization for Standardization 27002)?	❑ Yes ❑ No If yes, describe and provide relevant documentation. _____
63.	Does supplier conduct security audits (e.g., Statement on Auditing Standards 70 Type 2 audits)?	❑ Yes ❑ No If yes, describe the audit process and frequency, and provide the most recent audit report. _____
64.	Describe and attach any documentation that you feel would assist in this supplier assessment.	

For Internal Use Only: (Electronic/typed signature acceptable)

Data privacy determination:	❑ Approved ❑ Denied ❑ Need more information	
Determination made by:	_____ Cyber Security Representative	_____ Date
Security level allowed:	❑ Confidential Information ❑ Confidential Restricted Information ❑ PHI ❑ Credit or Debit Card Number ❑ n/a – not Data Privacy relevant	
Approved by:	_____ Business Unit Project Manager	_____ Date

Appendix G. Source Documents

Sector Documents

- *Cybersecurity Procurement Language for Energy Delivery Systems*, Washington, D.C.: U.S. Department of Energy, Energy Sector Control Systems Working Group, 2014
- *Dams Sector: NIST Cybersecurity Framework Implementation Guidance*, to be released in 2016
- *Dams Sector Roadmap to Secure Control Systems*, Washington, D.C.: U.S. Department of Homeland Security, 2010
- *Dams Sector Security Guidelines*, Washington, D.C.: U.S. Department of Homeland Security, 2015
- *Dams Sector-Specific Plan: An Annex to the NIPP 2013*, Washington, D.C.: U.S. Department of Homeland Security, 2015
- *Energy Sector Cybersecurity Framework Implementation Guidance*, Washington, D.C.: U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, 2015
- *Principles and Resources for Managing Supply Chain Cybersecurity Risk*, Washington, D.C.: Edison Electric Institute, 2015

Federal Agency Guidelines

- *Critical Infrastructure Protection Reliability Standards*, Washington, D.C.: North American Electric Reliability Corporation (NERC), 2016
- *Electricity Subsector Cybersecurity Risk Management Process*, Washington, D.C.: U.S. Department of Energy, 2012
- *FERC Security Program for Hydropower Projects: Revision 3*, Washington, D.C.: Federal Energy Regulatory Commission, Division of Dam Safety and Inspections, 2015
- FERC FAQ for Security Program for Hydropower Projects, to be released in 2016
- *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*, Gaithersburg, MD: National Institute of Standards and Technology, 2014
- *Pipeline Security Guidelines*, Washington, D.C.: Transportation Security Administration, 2011
- *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*, Washington, D.C.: North American Electric Reliability Corporation (NERC), 2010
- *Security Guideline for the Electricity Sector: Protecting Sensitive Information*, Washington, D.C.: North American Electric Reliability Corporation (NERC), 2012

NIST Computer Security Special Publications:

- *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (NIST 800-53A), Gaithersburg, MD: National Institute of Standards and Technology, 2014
- *Computer Security Incident Handling Guide* (NIST 800-61), Gaithersburg, MD: National Institute of Standards and Technology, 2012
- *Contingency Planning Guide for Federal Information Systems* (NIST 800-34), Gaithersburg, MD: National Institute of Standards and Technology, 2010
- *Guide for Conducting Risk Assessments: Revision 1* (NIST 800-30), Gaithersburg, MD: National Institute of Standards and Technology, 2012
- *Guide to Industrial Control Systems (ICS) Security* (NIST 800-82), Gaithersburg, MD: National Institute of Standards and Technology, 2011

- *Managing Information Security Risk: Organization, Mission, and Information System View* (NIST 800-39), Gaithersburg, MD: National Institute of Standards and Technology, 2011
- *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (NIST 800-171), Gaithersburg, MD: National Institute of Standards and Technology, 2014
- *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST 800-53), Gaithersburg, MD: National Institute of Standards and Technology, 2013
- *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (NIST 800-161), Gaithersburg, MD: National Institute of Standards and Technology, 2015

NIST Cybersecurity Practice Guides:

- *IT Asset Management* (NIST 1800-5), Gaithersburg, MD: National Institute of Standards and Technology, 2015

Homeland
Security