Roadmap to Secure Control Systems in the Dams Sector

November 2015

National Protection and Programs Directorate
Office of Infrastructure Protection
Sector Outreach and Programs Division

Homeland Security

Page intentionally left blank

CONTENTS

FOREWORD

The *Roadmap to Secure Control Systems in the Dams Sector* (Roadmap) describes a plan for voluntary improvement of cybersecurity in the Dams Sector. Control systems roadmaps provide an opportunity for industry experts to offer opinions concerning the state of control systems cybersecurity and to recommend strategies for improvement within the Sector. This Roadmap brings together Dams Sector stakeholders, including government agencies and owners and operators, with a common set of goals and objectives. It also provides milestones on which to focus specific efforts and activities for achieving the goals over the next 10 years, while addressing the Dams Sector's most urgent challenges, longer-term needs, and practices for reducing cybersecurity risk to control systems.

The Office of Infrastructure Protection and the Office of Cybersecurity and Communications within the U.S. Department of Homeland Security facilitated the development of this Roadmap with volunteers from Dams Sector and industry stakeholder organizations. This Roadmap provides a beginning point and a template for action as industry and government work together to achieve a common objective for securing control systems within the Dams Sector.

ACKNOWLEDGMENTS

The U.S. Department of Homeland Security, Office of Infrastructure Protection, Sector Outreach and Programs Division, Dams Sector-Specific Agency would like to acknowledge the Dams Sector Council members for their valued contributions in the development of the *Roadmap to Secure Control Systems in the Dams Sector*.

IP Cover Photo Location: The Dalles Dam, Oregon

EXECUTIVE SUMMARY

The *Roadmap to Secure Control Systems in the Dams Sector* (Roadmap) describes a plan and strategic vision for voluntary improvement of the cybersecurity posture of control systems within the Dams Sector. Designing, operating, and maintaining a facility to meet essential reliability, safety, and security needs requires careful evaluation and analysis of all risk factors including physical, cyber, and human. The interaction of both internal and external processes and business systems must also be considered. A cyber event, whether caused by an external adversary, an insider threat, or inadequate policies and procedures can initiate a loss of system control resulting in negative consequences. This Roadmap recognizes this interconnectivity, but restricts its scope by addressing only the cyber issues of control systems.

Many of the control systems used today were designed for operability and reliability during an era when there were fewer security concerns than there are today. These systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and/or communications technologies. Infiltrating and compromising these systems often required specific knowledge of individual system architectures and physical access to system components. Today's control systems are highly network-based and use common and open communication protocols; this provides interoperability, but also has the potential to expose network assets to cyber infiltration and subsequent manipulation of sensitive operations.

Challenges to cybersecurity consist of the direct risk factors that increase the probability of a successful cyberattack and the factors that limit the ability to implement ideal security enhancements. Many owners and operators within the Dams Sector do not have adequate inventories of their critical assets and associated control systems or a good understanding of the risks (threats, vulnerabilities and consequences) of a cyberattack. The growing number of nodes and access points has also made identifying vulnerabilities more complex. Widely accepted industry standards, consistent metrics, and reliable measuring tools are not readily available.

Some control systems have poorly designed connections between control systems and enterprise networks, use unauthenticated command and control data, and do not provide adequate access control for remote access points. Security improvements for legacy systems are limited by the existing equipment and architectures that may not be able to accept security upgrades without degrading performance.

An additional challenge is a lack of information sharing among owners and operators and other cyber stakeholders regarding cybersecurity threats, events, and their consequences due to concerns as to how that information will be used, disseminated, and protected. Possibly, as a result of this lack of information sharing, the return on investment is unclear for vendors who sustain control system and security tool improvement, including research and development (R&D) to advance the technology. A further complication is that vendors currently do not have adequate requirements or standards to design, build, and maintain cybersecurity for control systems. Evolving cyber threats, changes in cyber-intrusion technologies, and developments in information technology can pose challenges to building security into control systems with long life spans.

While Sector partners actively manage the risk to their operations through monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions, increasingly sophisticated threats require a more thorough examination of risks associated with cybersecurity.

The control systems roadmap provides an opportunity for the Dams Sector community to identify its concerns, communicate recommended strategies for improvement, and provide a venue for government assistance. It also provides the Dams Sector with specified milestones on which to focus specific efforts and activities to achieve key goals over the next 10 years, while addressing the Sector's most urgent challenges, which include developing mitigating solutions, defining longer-term needs, and articulating control system security guidelines and practices for improvement.

1. INTRODUCTION

Leaders from the Nation's critical infrastructure sectors and government agencies recognize the need to plan, coordinate, and focus ongoing efforts to improve control system security. They agree that a concise plan, with specific goals and milestones for implementing security across individual sectors, is required to prioritize critical needs and gaps to assist critical infrastructure owners and operators in reducing the risk of future cyberattacks on control systems. The need to address the risks associated with cyber systems has prompted Dams Sector partners to step forward and collaborate on a unified cyber and control systems security strategy to address the most significant issues and concerns regarding cybersecurity and control systems within the Dams Sector, including the criticality of control systems in all areas related to dam operations.

In recent years, roadmaps have been developed to guide the efforts of individual sectors in securing their control systems. Roadmaps provide appropriate strategies for securing their sectors and an opportunity for industry and government experts within a sector to collectively address issues concerning the state of control system cybersecurity. The U.S. Department of Homeland Security (DHS) is leveraging this industry perspective to help the sector stakeholder community develop programs and risk mitigation measures that align with the sector's plan. In addition to owners and operators, other sector stakeholders (including control system vendors, system integrators, and academia) can use these roadmaps to map supporting activities with industry.

Because the Roadmap goals are voluntary, implementation of the ideas and concepts presented in this document are addressed based on the organization's overall cybersecurity policies and procedures. Still, roadmaps are recognized as quality documents that provide excellent descriptions of control systems risk challenges and general methods for improving the security of control systems over the ensuing decade.

This Roadmap provides a comprehensive framework and recommended strategies focused on the protection of control systems across the Dams Sector. This framework will enhance the Sector's understanding and management of cyber risks, facilitate the identification of practical risk mitigation solutions, and promote information sharing and improve Sector-wide awareness of cybersecurity concerns. In addition, the Roadmap will guide the Sector in developing a more refined understanding of common vulnerabilities; potential consequences; and the programs, outreach, and research efforts that can assist in developing and implementing cost-effective risk management and mitigation strategies. Specific control systems security goals and corresponding milestones were established in response to those challenges and are detailed in Section 3 of this Roadmap.

ROADMAP PURPOSE

This Roadmap builds on existing government and industry efforts to improve the security of control systems within the Dams Sector.

Roadmap Purpose

- **Present the Dams Sector's security vision**
- **Define a consensus-based strategy for the Sector**
- **Propose a comprehensive plan to improve security**
- **Encourage stakeholder participation and compliance**
- **Guide industry, academia, and government effort**
- **Identify opportunities for cross-sector cooperation**
- **Promote continuous improvement in security posture**
- **Strengthen government programs to improve protection**
- **Support implementation of goals in the Dams Sector-Specific Plan**

The Roadmap is intended to help coordinate and guide related control system security efforts within the Dams Sector and highlight recommended strategies to address the Sector's most urgent challenges, mitigation requirements, and long-term research and development (R&D) needs. This Roadmap will provide a strategic vision to improve the cybersecurity posture of control systems within the Sector, by defining a common strategy that addresses the needs of owners and operators.

This Roadmap:

- Presents the Dams Sector's cybersecurity vision, along with a supporting outline of goals and milestones, to improve the cybersecurity posture of control systems within the Sector;
- Defines a consensus-based strategy that addresses the specific cybersecurity needs of owners and operators within the Sector;
- Proposes a comprehensive plan for improving the security, reliability, and functionality of control systems;
- Proposes methods and programs that encourage participation of all stakeholders;
- Guides industry, academia, and government efforts to improve cybersecurity;
- Identifies opportunities for cooperative work across sectors in cybersecurity awareness, training, and information sharing;
- Promotes continuous improvement in the cybersecurity posture of control systems within the Sector; and
- Supports the implementation of the goals described in the Dams Sector-Specific Plan related to cybersecurity and control systems.

ROADMAP SCOPE

This Roadmap addresses cybersecurity issues related specifically to control systems owned and operated by Dams Sector partners whose facilities are part of the Nation's critical infrastructure. The functional and organizational composition of critical infrastructure sectors is defined in the *National Infrastructure Protection Plan* (NIPP) and associated Sector-Specific Plans (SSPs).

Designing, operating, and maintaining a facility which meets essential reliability, safety, and security needs requires the careful evaluation and analysis of all risk factors including physical, cyber, and human. The interaction of both internal and external process and business systems must also be considered. Attacks on a cyber system may involve only the cyber components and their operation; but those impacts may extend into the physical, business, human, and environmental systems to which they are connected. A cyber event (whether caused by an external adversary, an insider threat, or inadequate policies and procedures) can initiate a loss of system control, resulting in negative consequences. This Roadmap recognizes this interconnectivity, but restricts its scope by addressing only the cyber issues of control systems. Interactions with physical, business, and safety systems (and their security components) are an accepted reality necessitating the appropriate coordination of interfaces for secure and reliable operation.

Cyber risk to control systems encompasses elements of the business network and the Internet to the extent that they are connected to control systems. Since this Roadmap focuses on control systems, securing access to and control of the business network and the Internet is outside the scope of this Roadmap. While security for IT systems is outside the scope of this Roadmap, interfaces between the Industrial Control Systems (ICS) networks, business system networks, and the Internet must be coordinated to ensure proper application of security measures and responsibilities.

Physical access to cyber systems is also a significant contributing factor in cyber risk. Similarly, physical damage and life safety issues resulting from cyber compromise are some of the principal factors contributing to control systems risk. This Roadmap considers all of these factors in understanding and planning for cybersecurity enhancements. However, describing physical access control and physical consequence management is outside the scope of this Roadmap.

This Roadmap recommends goals, milestones, and needs over the near- (0–2 years), mid- (2–5 years), and long- (5-10 years) terms. Security needs encompass R&D, new technologies, systems testing, training and education, accepted industry practices, standards and protocols, policies, information sharing, and outreach and implementation. The Roadmap will be periodically updated to meet changing needs and to accommodate the dynamic nature of cybersecurity for control systems.

National Context

The U.S. Department of Homeland Security (DHS) leads the Federal Government's efforts to secure our Nation's critical infrastructure by working with owners and operators to prepare for, prevent, mitigate, and respond to threats. While DHS plays a central role, the Department cannot do this work alone. Public-private partnerships are essential. It is through partnerships that the Department continues to see value and positive impact in mitigating and rapidly responding to crises.

Facing threats to our Nation's critical infrastructure from cyberattacks that could disrupt our power, water, communications, and other critical infrastructures, the President issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*. These two reinforce the need for holistic thinking about security and risk management. Implementation of the EO and PPD will not only drive action toward system and network security and resiliency, but will also enhance the efficiency and effectiveness of the U.S. Government's efforts toward a more secure and resilient critical infrastructure.

Appendix B summarizes national policy guidance on securing cyber control systems.

Dams Sector Context

The Dams Sector operates under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a forum for government and private sector partners to engage a broad spectrum of activities to support and coordinate critical infrastructure security. The CIPAC consists of a Sector Coordinating Council (SCC) and a Government Coordinating Council (GCC).

SCCs are self-organized, run, and governed by industry organizations that represent a spectrum of key stakeholders within a sector. Within the Dams Sector, the Dams SCC serves as the private sector interface with the Federal Government on issues related to the security of dams, locks, and levees. Its primary purpose is to determine the nature of risks posed against Sector assets so that appropriate and timely information, as well as mitigation strategies, can be provided to the entities responsible for the operation and protection of those assets. The SCC also serves as the principal asset owner interface with other critical infrastructure sectors, as well as with DHS, the Federal Energy Regulatory Commission (FERC), and other government bodies, including the Dams GCC.

The GCC acts as the government counterpart and partner to the SCC in planning, implementing, and executing sector-wide security programs for the Sector's assets. It is comprised of representatives from various levels of government (Federal, State, local, and tribal), including Federal owners and operators, and State and Federal regulators of Sector assets. Its primary activities include identifying issues that require public-private coordination and communication; bringing together diverse Federal and State interests to identify and develop collaborative strategies that advance critical infrastructure protection; assessing needs and gaps in plans, programs, policies, procedures, and strategies; acknowledging and recognizing successful programs and practices; and leveraging complementary resources within government and between government and industry.

In addition, the DHS Office of Cybersecurity and Communications (CS&C) established the Control Systems Security Program (CSSP) in 2004, which is chartered to work with control systems security stakeholders through awareness and outreach programs that encourage and support coordinated control systems security enhancement efforts. In December 2008, the CSSP also established the Industrial Control Systems Joint Working Group (ICSJWG) as a coordination body to facilitate the collaboration of control systems stakeholders and to accelerate the design, development, and deployment of enhanced security for control systems.

In compliance with Homeland Security Presidential Directive 7 (HSPD-7) and PDD-21, the Dams Sector is also required to develop and maintain a Sector-Specific Plan (SSP) that details the Sector's plans to protect human resources, cyber systems, and physical assets. The *Roadmap to Secure Control Systems in the Dams Sector* provides a logical and cohesive framework to design and implement a strategy for carrying out the goals of the Dams SSP.

Appendix B summarizes national policy guidance on securing cyber control systems.

ACTION PLAN

This Roadmap proposes a strategic framework for investing in control system security, and for industry and government to act toward improving defenses against cyber events that would disrupt operations. It identifies the challenges and activities that should be addressed and outlines specific milestones that should be met over the next 10 years to reach the outlined goals and vision. While it contains many actionable items, it represents a strategic plan to the extent that financial resources are available and leadership is enabled to translate these priorities and milestones into productive projects, activities, and products.

2. CONTROL SYSTEM LANDSCAPE

The Dams Sector comprises dam projects, hydropower plants, navigation locks, levees, dikes, hurricane barriers, industrial waste (e.g. mine tailings) impoundments, or other similar water control facilities. Within the Dams Sector, control systems are used either onsite or remotely to control and/or monitor the operations of these structures. A control system is a device or group of devices that monitor, manage, command, direct, or regulate the behavior of other devices or group of devices. Typically, a control system will collect information about the operations taking place within the project as well as the status of the components in the facilities, such as gate position, reservoir level, hydroelectric generator output, and water flowrate. This information is then converted into electrical signals for processing and, if needed, enables corrective actions to be taken automatically or with human intervention.

Within the Dams Sector, the term “control system” is frequently used interchangeably with the term “Industrial Control System” (ICS). ICS is a general term that encompasses several types of control systems and, for the purpose of this Roadmap, is defined as the facilities, systems, equipment, services, and diagnostics that provide the functional monitoring, control, and protection capabilities necessary for effective and reliable operation. In some cases, an ICS may be comprised of non-electronic relay-based components without cyber assets connected to them, which, therefore, have a low risk of being affected in the occurrence of a cyber event. An electronic security system that protects an ICS can be considered an ICS itself if it is used to remotely monitor and control security equipment such as gates, barriers, and other access control systems.

Many of the ICSs used today were designed for operability and reliability during an era when there were fewer security concerns than there are today. These systems operated in fairly isolated environments and typically relied on vendor-specific or proprietary software, hardware, and/or communications technologies. Infiltrating and compromising these systems often required specific knowledge of individual system architectures and physical access to system components.

In contrast, modern ICSs are highly network-based and use common and open communication protocols; many controllers are also Internet Protocol (IP) addressable. Owners and operators have gained immediate benefits by extending the connectivity of their ICS. They have increasingly adopted commercial off-the-shelf (COTS) technologies that provide the higher levels of interoperability required among today’s modern infrastructures. Standard operating systems such as Windows or UNIX are increasingly being used in central supervisory stations that are typically connected to remote controllers via private and/or public networks provided by telecommunications companies. In addition, common telecommunications technologies such as the Internet, public-switched telephone networks, cable, or wireless networks are often used.

A typical SCADA system configuration is shown below in Figure 1. The left end of the figure shows the control center with its Local Area Network (LAN)-connected workstations, servers, and routers. The control center receives information from field locations and decides whether or not to act upon that information. If actions are to be taken, they are made possible through the use of remote controlled actuators at the field locations (right end of the figure). These actuators are controlled through signals which may be sent from the control center through wired communication lines or through radio, microwave, cellular, or satellite transmissions as indicated by the center of the figure.

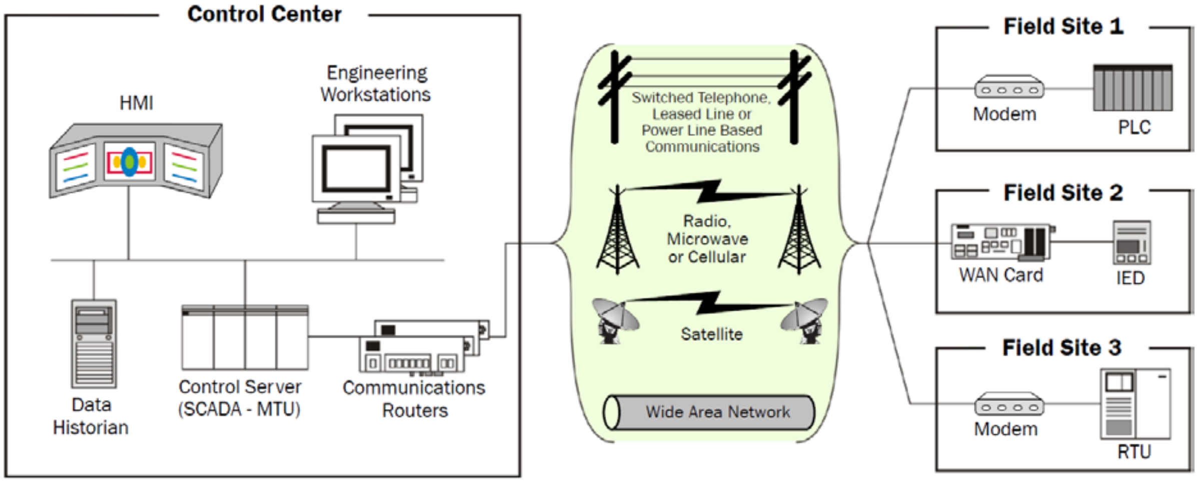


Figure 1. SCADA System General Layout (Stouffer et al., 2008)

The potential for system accessibility resulting from this interoperability exposes network assets to cyber infiltration and subsequent manipulation of sensitive operations. Furthermore, increasingly sophisticated cyberattack tools can exploit flaws in COTS components, telecommunication methods, and common operating systems found in modern control systems. The ability of owners and operators to discover and understand such emerging threats and system vulnerabilities is a prerequisite to developing effective security polices and countermeasures.

Even though ICSs are quite reliable, security policies and practices are often undependable. Detailed analyses of potential threats and associated consequences are also lacking in some facilities. As operating practices have evolved to allow real-time operation and control of critical assets, protecting ICSs from cyber risks has become more difficult. Some of the most serious security issues inherent in current ICSs, related to increased ICS vulnerabilities include:

Protection Issues

- **Increased connectivity**
- **Interdependencies**
- **Complexity**
- **Legacy systems**
- **Remote Access**
- **Cloud computing**
- **Wireless connection**
- **Offshore reliance**
- **Information availability**

- **Increased Connectivity** - Today’s ICSs are increasingly connected to company business systems that rely on common operating platforms and are accessible through the Internet. Even though these changes improve operability and increase information dissemination, they also create serious cybersecurity vulnerabilities in those platforms. When company business systems share trusted interconnections with third-party systems, such as contractor or vendor systems, the vulnerabilities greatly increase.

- **Interdependencies -** Due to the high degree of interdependency among infrastructure sectors, failures within one sector can spread to others. A successful cyberattack may be able to take advantage of these interdependencies and produce cascading effects and amplify the overall virtual, physical, and economic damage.

- **Complexity -** The demand for real-time monitoring or control has increased system complexity in several ways. Access to ICSs is being granted to more users, business systems and ICSs are interconnected, and the degree of interdependency among infrastructures has increased. Dramatic differences in the training and concerns of those in charge of IT systems and those responsible for control system operations have also led to challenges in coordinating network security between these two key groups.

- **Legacy Systems -** Although older legacy supervisory control and data acquisition (SCADA) systems may operate in more independent modes, they tend to have inadequate password policies and security administration; no data protection mechanisms; and protocols that are prone to snooping, interruption, and interception. These insecure legacy systems have long service lives and will remain vulnerable for years to come unless these problems are mitigated.

- **Remote Access -** Even limited connection to the Internet exposes ICSs to all of the inherent vulnerabilities of interconnected computer networks including viruses, worms, hackers, and terrorists. Control channels that use wireless or leased lines that pass through commercial telecommunications facilities may also provide minimal protection against forgery of data or control messages. These issues are of particular concern in industries that rely on interconnected business and control networks with remote access from within or outside the company. Virtual Private Network (VPN) technology is increasingly being used by organizations to give employees secure remote access to their computing and control resources. However, malicious actors continually look for weaknesses in VPN implementation and develop methods to circumvent VPN security and gain remote access to control systems and networks.

- **Cloud Computing -** Using a network of remote servers hosted on the Internet to store, manage, and process data rather than a local server or a personal computer can introduce elements of risk. The use of cloud computing with industrial control processes is becoming more common. A Dams Sector organization should perform a risk assessment when considering using cloud computing for any of its processes.

- **Wireless Connection -** A type of data communication that is performed and delivered wirelessly. This is a broad term that incorporates all procedures and forms of connecting and communicating between two or more devices using a wireless signal through wireless communication technologies and devices. Wireless communication generally works through electromagnetic signals that are broadcast by an enabled device within the air, physical environment, or atmosphere. The sending device can be a sender or an intermediate device with the ability to propagate wireless signals. The communication between two devices occurs when the destination or receiving intermediate device captures these signals, creating a wireless communication bridge between the sender and receiver device. Wireless communication has various forms, technology, and delivery methods including:

    - Satellite
    - Mobile (Cellular)
    - Wi-Fi network
    - Infrared
    - Bluetooth

  Although all of these communication technologies have different underlying architectures, they all lack a physical or wired connection between their respective devices to initiate and execute communication.

- **Offshore Reliance -** There are no feasible alternatives to the use of COTS products in ICSs. Many software, hardware, and control system manufacturers are under foreign ownership or develop systems in countries whose interests do not always align with those of the United States. Also of concern is the practice of contracting ICS support, service, and maintenance to third parties located in foreign countries.

- **Information Availability -** Information that would aid a potential attacker is widely available and easily accessible via Internet searches. The sources of this information may range from manuals and training videos on ICSs; National SCADA Test Bed reports regarding common SCADA vulnerabilities; and malicious information on the Internet that describes particular vulnerabilities, including how to exploit them. This issue is exacerbated by the increasing use of COTS products and the prevalence of common operating systems found in modern control systems.

Known cybersecurity threats that affect ICSs include:

- **Increased Use of Digital Controls -** Replacement of analog and electro-mechanical controllers with digital and/or microprocessor-based controllers has caused increased exposure to cyber threats.
- **Supply Chain -** Vendor access to ICSs has not always included procedures for granting authorized personnel logical access to systems. Systems may be inherently vulnerable as a result of programming errors.
- **System Updates -** System updates and patches available on some manufacturer and vendor Websites have been known to contain malware. Proper patch management may be difficult if not readily accessible from the vendor due to ICS network isolation. In addition, patching may be hindered by ICS network high availability requirements.
- **Removable Data Storage Devices -** Increased use of portable devices capable of transferring data can bypass network defenses and exploit potential vulnerabilities.
- **Insider Threats -** Systems are increasingly susceptible to insider threats including social engineering attacks, disgruntled employees, and intentional or unintentional actions.

A more in-depth description of typical ICSs and their vulnerabilities and currently available general security enhancements can be found on the United States Computer Emergency Readiness Team (US-CERT) Control System Website at http://www.us-cert.gov/control_systems/csvuls.html, as well as The National Institute of Standards and Technology Special Publication 800-82, "*Guide to Industrial Control Systems (ICS) Security, Recommendations of the National Institute of Standards and Technology*."

KEY STAKEHOLDERS

ICS security is a responsibility shared by owners and operators, vendors, and stakeholders who manage and govern critical infrastructure assets. The ICS stakeholder community also includes government agencies, industry organizations, commercial entities, and researchers, each of which brings specialized skills and capabilities for improving control system security and protecting critical infrastructure. Key stakeholder groups and sample members include:

- **Asset Owners and Operators** strive to ensure that ICSs are secure by making appropriate investments, reporting threat information to the government, and implementing protective practices and procedures;
- **Federal, State, Local, Tribal, and Territorial Agencies** securely share threat information and collaborate with industry to identify and fund gaps in ICS security research, development, and testing efforts;
- **Industry Organizations** provide coordination and leadership across multiple sectors to help address important barriers, form partnerships, and help to develop standards and guidelines specific to the needs of their sector membership;
- **Commercial Entities**, such as system and software vendors and system integrators, develop and deliver control system products and services to meet the security needs of owners and operators;
- **R&D Organizations** are funded by government and industry to explore long-term security solutions, develop new tools, and address solutions for ICS system vulnerabilities, hardware, and software; and
- **Universities and Colleges** are chartered to provide education for future generations and ideally provide courses and degrees that satisfy the needs and requests of industry.

AN APPROACH FOR SECURING CONTROL SYSTEMS

Protecting infrastructure ICSs is a formidable challenge requiring a comprehensive approach that addresses the urgent security concerns of today’s systems while preparing for the needs of tomorrow. Owners and operators must understand and manage cyber risks, secure their legacy systems, apply security tools and practices, and consider new control system architectures—all within a competitive business environment. Government has a large stake in the process because infrastructure sectors are critical to national security and have interdependencies that could result in cascading impacts during a cyber event. Still, cybersecurity enhancements must compete with other investment priorities, and many executives find it difficult to justify security expenditures without a strong business case. Sector-specific roadmaps play an essential role in supporting the national strategy to articulate the essential goals for improving control system security and to align and integrate the efforts of industry and government to achieve those goals.

The Roadmap presents an approach that consists of establishing a vision, defining top-level goals aimed at achieving that vision, and then identifying the challenges associated with the goals. Milestones are then identified that, if implemented and successful, will address challenges and assist in meeting goals.

VISION

The vision of the Dams Sector with respect to control systems security is:

> *Control systems throughout the Dams Sector will be able to operate securely, robustly, resiliently, and protected at a level commensurate with risk. Control systems throughout the Dams Sector will be able to operate with no loss of critical function in vital applications during and after a cyber event without impacting the overall mission of the project.*

It is envisioned that the Roadmap will serve as an initial approach and mechanism to provide owners and operators with goals, recommendations, and guidelines focused on enhancing control systems security to a level at which risk is tolerable and at which the Dams Sector is able to function in a cost-effective and rational manner to mitigate dams cybersecurity events as appropriate.

CONTROL SYSTEMS SECURITY GOALS

Today’s ICSs have become an essential element in the management of complex processes and production environments. The risk of exploitation by physical or cyber means with the intent to cause harm is real and can have negative impacts on an asset owner’s business, public safety, the environment, and national security. Owners and operators within the Nation’s critical infrastructure must understand and manage this risk by securing their installed systems, conducting vulnerability assessments, employing security tools and practices, and considering security as they procure and install next-generation systems.

Based on previous efforts in the Energy, Water, and Chemical Sectors, five general goals have been selected as the guiding objectives of this Roadmap. These goals are structured after classical security models that measure, assess, protect, detect, defend (detain or eliminate as may be required), recover, and build-in security (rather than attaching it as an after-thought), as well as provide continual improvement. They are also constructed in a classic problem-solving pattern— identify the problem, establish a problem solving methodology, solve the problem, and evaluate the problem for the future to ensure continued remediation as appropriate. The first three goals are technical; the fourth encompasses programmatic, management, and cultural achievements; and the fifth encourages and facilitates a partnership between owners and operators and ICS vendors to make security an integral part of the specified and developed systems.

Goal 1: Measure and Assess Security Posture - Companies and operational entities will have a thorough understanding of their current security posture to determine where control system vulnerabilities exist and what actions may be required to address them. It is recommended that owner/operators perform ongoing security monitoring of their control system networks with timely mitigation of identified vulnerabilities.

Goal 2: Develop and Integrate Protective Measures - As security problems are identified or anticipated, protective measures will be developed and applied to reduce system vulnerabilities, system threats, and their consequences. Examples of security measures that can be incorporated into the system during the design phase are:

- Isolating the control system from all other business or commercial electronic communications mechanisms as recommended by best practices;
- Utilizing unidirectional data gateways (e.g. Data Diodes);
- Employing secure file transfer solutions;
- Using appropriate communications protocols/firewalls/demilitarized zones for external connectivity; and
- Limiting system protocols and services to those that are absolutely necessary for system functionality.

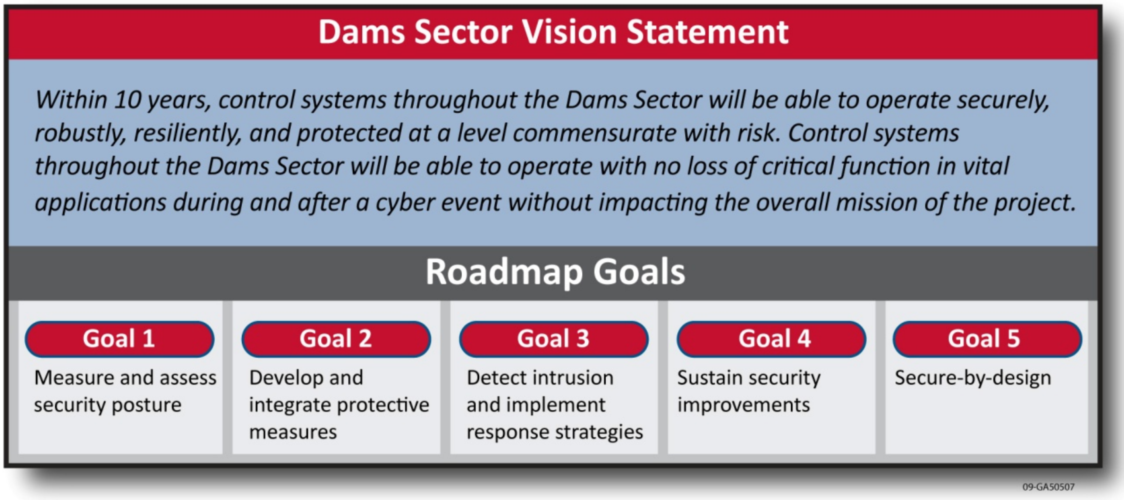
Appropriate security solutions should be devised by the Sector, as well as vendors and R&D organizations outside the Sector; however, legacy systems will be constrained by the inherent limitations of existing equipment and configurations. As legacy systems age, these should be replaced or upgraded with next-generation control system components and architectures that offer built-in, end-to-end security. This replacement is typically not driven solely by security-related concerns.

Goal 3: Detect Intrusion and Implement Response Strategies - Cyber intrusion tools are sophisticated to the degree that any system vulnerability can be exploited without much difficulty unless adequate protections are implemented. The Sector should be operating networks that automatically provide contingency and remedial actions in response to attempted intrusions.

Goal 4: Sustain Security Improvements - Maintaining aggressive and proactive cybersecurity of ICSs over the long term will require a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders. The Dams Sector owners and operators should collaborate within the Sector, across sectors, and with government to remove barriers to progress and create policies that accelerate and sustain advancement in securing their ICSs.

Goal 5: Secure-by-Design - Dams Sector owners and operators should insist, through specifications and orders, that vendors provide systems that are secure-by-design and should work with vendors to achieve this goal.

These goals provide a logical approach for organizing the collective efforts of industry, government, and other key stakeholders to achieve the vision.



Dams Sector Vision Statement

Within 10 years, control systems throughout the Dams Sector will be able to operate securely, robustly, resiliently, and protected at a level commensurate with risk. Control systems throughout the Dams Sector will be able to operate with no loss of critical function in vital applications during and after a cyber event without impacting the overall mission of the project.

Roadmap Goals

Goal 1	Goal 2	Goal 3	Goal 4	Goal 5
Measure and assess security posture	Develop and integrate protective measures	Detect intrusion and implement response strategies	Sustain security improvements	Secure-by-design

DAMS SECTOR PERSPECTIVES

This section addresses issues specific to the Dams Sector that have an impact on potential security solutions.

BACKGROUND

As previously referenced, the NIPP provides the unifying structure for the integration of critical infrastructure security and resilience efforts as part of a coordinated national program. The NIPP includes 17 SSPs that detail the application of the overall risk management framework to each specific sector.

According to the Dams SSP, the Dams Sector comprises dam projects, hydropower plants, navigation locks, levees, dikes, hurricane barriers, mine tailings and other industrial waste impoundments, or other similar water retention and water control facilities. Dam projects are complex facilities that may include multiple water impoundment or control structures, reservoirs, spillways, outlet works, powerhouses, and canals or aqueducts. In some cases, navigation locks are also part of the dam project. Levees can also be systems with multiple components that include embankment sections as well as floodwall sections, pumps and pumping stations, interior drainage works, closure structures, penetrations, and transitions.

The Dams Sector is a vital and beneficial part of the Nation’s infrastructure and continuously provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.

Examples of the benefits derived from Sector assets are discussed below.

- **Water Storage and Irrigation -** Dams create reservoirs throughout the United States that supply water for a multitude of industrial, municipal, agricultural, and recreational uses. Ten percent of America’s crop production is irrigated by water stored behind dams, and thousands of jobs are associated with irrigated crops production.
- **Electricity Generation -** The United States is one of the largest producers of hydropower in the world, second only to Canada. Dams in the United States have a capacity base of 79 gigawatts (GW), or 101 GW when including contributions from pumped storage facilities—contributing 7 percent of the Nation’s electricity, and representing 52 percent of the Nation’s renewable energy generation.
- **“Black Start” Capabilities -** A black start is the process of restoring a power station to operation without the need of external power. Hydroelectric plants are often designated as black-start power sources because they need very little electricity to start and can supply electricity to start up other power stations. During the August 2003 blackout in the Northeast, hydropower projects in New York and several other States were able to quickly start generating electricity, leading the way to restoring power to millions of American homes and businesses.
- **Recreation -** Dams and other sector assets provide prime recreational facilities throughout the United States. In 2002, a total of 105.7 million recreation user days and nights were assessable at hydropower facilities licensed by the Federal Energy Regulatory Commission (FERC). In addition, about 400 million people annually visit a facility of the U.S. Army Corps of Engineers (USACE), and about 90 million visit a facility of the Bureau of Reclamation (Reclamation) in a year.
- **Navigation -** Navigation projects constitute an essential component of the U.S. waterway system, which includes 236 lock chambers at 192 lock sites owned and/or operated by the USACE. A principal value of the inland and intra-coastal navigation system is the ability to efficiently transport large volumes of bulk commodities moving long distances. In 2013, 566.7 million tons of waterborne cargo transited the inland waterways, a volume equal to roughly 14% of all

intercity freight and transportation services valued at nearly $216 billion. The ability to move more cargo per shipment makes barge transportation both fuel efficient and environmentally advantageous.

- **Flood Risk Reduction -** Many dams and levees function as flood control projects, thereby reducing the potential human health and economic impacts of flooding. Reservoirs and levees built by USACE reportedly prevented more than $19 billion in potential damages during the 1993 Midwest Flood. USACE levee systems currently provide a 6:1 return ratio on flood damages prevented compared to initial costs; robust levee systems provide a 24:1 return ratio on investments. Levees and hurricane barriers reduce flood damages to rural communities as well as major metropolitan areas.
- **Sediment Control -** Some dams enhance environmental protection by controlling detrimental sedimentation.
- **Impoundment of Mine Tailings and Industrial Waste Materials -** More than 1,500 mine tailings and industrial waste impoundments controlled by dams in the Nation facilitate mining and processing of coal and other vital minerals and manufacturing while protecting the environment.

As with all critical infrastructure, the technological and national security environment in which the dam infrastructure is operated and maintained continues to evolve. New threats to the continued reliability and integrity of all infrastructure require vigilance.

While many dam projects are required to allow access to areas surrounding their facilities, including the dam and navigational lock operations area, and may even encourage public visits and guided tours, primary access roads to the generation facility and/or control center are secured. In addition, the area outside the facility's perimeter is open to the public for viewing, and recreational access is provided for boating and fishing. As a result, dam owners and operators actively manage the risk of human access through monitoring and mitigation activities. However, increasingly sophisticated threats are requiring a more thorough examination of cyber risk.

Due to the high degree of interdependency among infrastructure sectors, a successful cyberattack within one or more sectors can possibly impact other sectors amplifying potential overall physical, social, and economic damages. The following sectors are linked to the Dams Sector:

- The **Agriculture and Food Sector** depends on a continued source of water for irrigation and water management;
- The **Transportation Systems Sector** relies on dams and locks to manage inland waterways for navigation— roads are often located on dam crests;
- The **Water Sector** supplies potable water stored behind dams to concentrated populations and commercial facilities in the United States;
- The **Energy Sector** provides approximately seven percent of the Nation's power needs with hydropower dams; and
- The **Emergency Services Sector** relies on Dams Sector assets for firefighting water supply, emergency water supply, and waterborne access in the event of a significant disaster.[a]

The potential risks in the event of asset failures within the Dams Sector are considerable and could result in significant impacts (e.g., loss of life, massive property damage, long-term consequences). A successful cyberattack would affect dam operations in a variety of ways, some with potentially devastating repercussions. An attack could:

[a] U.S. Department of Homeland Security, Dams Sector-Specific Plan 2015, http://www.dhs.gov/publication/nipp-ssp-dams-2015, (Accessed 1/20/2016).

- Disrupt the operation of ICSs by delaying, blocking, or shutting down the flow of information, thereby denying availability to dam control system operators;
- Send false information to control system operators to disguise unauthorized changes, or to initiate inappropriate actions;
- Modify the system's software, producing unpredictable results; or worse, planned disruptive or dangerous results such as overtopping or large releases;
- Interfere with the operation of safety and protection systems, potentially resulting in damage to equipment;
- Make unauthorized changes to ICS set points, alarm thresholds, and control sequences resulting in premature shutdown of processes (e.g., shutting down generators, operating or disabling sluice and spillway gates, and control valves) or disable control and safety equipment;
- Interfere with the operation or security systems of interdependent projects; and
- Disrupt the reliability of Bulk Electric Systems (BES), flood control, water conveyance, or other services.

SECTOR REGULATIONS

In the United States, the safety of dams, levees, and other Dams Sector assets is regulated by Federal, State, local, and tribal agencies. Many facilities throughout the Dams Sector are multi-purpose and, therefore, must adhere to multiple standards corresponding to the different services the facility provides.

Due to the strong interface between the Dams Sector and hydroelectric power generation, it is necessary to briefly discuss the North American Electric Reliability Corporation (NERC). NERC is a self-regulatory organization subject to oversight by FERC and governmental authorities in Canada. In response to the northeastern blackout in 2003, FERC granted NERC the legal authority to enforce reliability standards with all North American users, owners, and operators of the BES and made compliance with those standards mandatory and enforceable. These standards focus on ensuring that all entities responsible for the reliability of the BES in the United States and Canada identify and protect critical cyber assets that control or impact the reliability of those systems. These standards are referred to as Critical Infrastructure Protection (CIP) Reliability Standards.[b]

The CIP standards are mandatory and require bulk power system users, owners and operators, and hydroelectric power plants in the United States to identify and document cyber risks and vulnerabilities, establish controls to secure critical cyber assets from physical and cyber sabotage, report security incidents, establish plans for recovery in the event of an emergency, and certify their level of compliance with the standards. Entities to which the standards apply are subject to NERC audits and fines for noncompliance.

OTHER CYBERSECURITY STANDARDS AND GUIDELINES

As part of the ongoing initiative to develop a unified information security framework for the Federal Government and its contractors, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 "*Assessing Security and Privacy Controls in Federal Information Systems and Organizations*" includes security controls for both national security and non-national security systems. The updated security control catalog incorporates best practices in information security from the U.S. Department of Defense, intelligence community, and civil agencies to produce the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems. The

[b] CIP-002 through CIP-009 has undergone several revisions since first approved. For additional information pertaining to the CIP Standards, access the NERC Website at http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. (Accessed 1/20/2016).

standardized set of management, operational, and technical controls provides a common specification language for securing Federal information systems which process, store, and transmit national security and non-national security information. The revised security control catalog also includes best practices for safeguards and countermeasures needed by organizations to address advanced cyber threats capable of exploiting vulnerabilities in Federal information and ICSs. In 2006, NIST also established the "*Industrial Control System Security Project*" to improve the security of public and private sector ICSs; a major part of the project is to research the applicability of SP 800-53 to ICSs, and to clarify/rectify any problems experienced in applying SP 800-53 to ICSs. The results of this effort may be seen in NIST SP 800-82 "*Guide to Industrial Control Systems Security.*"

NIST standards are mandatory for Federal facilities under the Federal Information Security Management Act of 2002 (FISMA) guidelines. FISMA 44 U.S.C. § 3541, et seq. was enacted as Title III of the *E-Government Act of 2002* (Pub. L. 107-347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for information and information systems.

In addition to developing new policy and technology solutions itself, the Sector will participate in national-level and cross-sector initiatives to identify new and existing solutions that may exist or be developed outside of the Dams Sector.

The CIP standards, from the owner and operator perspective, do not provide the most cost effective measures by requiring implementation of physical mitigations to "critical" cyber assets, as it is unclear as to what those "critical" cyber assets are. In addition, the CIP standards primarily focus on access control (both cyber and physical security) of a dam's hydropower features, rather than on the security of the dam itself. This represents a shift from cyber mitigation efforts to the physical mitigation of a cyber threat. It is very difficult for some dam owners to comply with all of the CIP standards since it may not always be feasible to implement a security perimeter around their cyber assets. Many owners and operators of hydropower facilities are more concerned with the possible consequences associated with a dam failure than with those of a hydropower plant shutdown caused by a cyberattack. This represents an overarching concern of the Sector since costly fines are levied for noncompliance with the standards.

Dams Sector Cybersecurity Coordination

As previously referenced, the NIPP heavily relies on the sector partnership framework as the primary organizational structure for coordinating critical infrastructure efforts and activities. As part of the partnership framework, the Dams Sector Council members conduct meetings on a quarterly basis to discuss the status of various ongoing collaborative efforts and initiatives focused on enhancing the physical, human, and cybersecurity of the Dams Sector, as well as to identify future requirements associated with the prevention, protection, security, and resilience of Sector assets.

Dams Sector Coordinating Council

The Dams Sector Coordinating Council (SCC) currently consists of the following industries, trade associations, and other dam stakeholders:

Ameren Services Company

American Electric Power

Association of State Dam Safety Officials (ASDSO)

Association of State Floodplain Managers (ASFPM)

Brookfield Renewable Energy

Consumers Energy (subsidiary of CMS Energy)

Colorado River Energy Distributors Association (CREDA)

Dominion Resources

Duke Energy Corporation

Exelon

Grant County Public Utility District

Miami Conservancy District / NAFSMA

National Association of Flood and Stormwater Agencies (NAFSMA)

National Hydropower Association (NHA)

National Water Resources Association

New York City - Department of Environmental Protection

New York Power Authority

Northwestern Energy

Ontario Power Generation

Pacific Gas & Electric Company

Salt River Project Agricultural Improvement and Power District

Scana Corporation

Seattle City Light

South Carolina Public Service Authority (Santee Cooper)

Southern California Edison

Southern Company (Generation)

Talen Energy

Xcel Energy Corporation

Dams Government Coordinating Council

The Dams Government Coordinating Council (GCC) currently consists of the following Federal, State, local, tribal, and territorial governments:

Bonneville Power Administration (BPA)

Environmental Protection Agency (EPA)

Federal Bureau of Investigation (FBI)

Federal Emergency Management Agency (FEMA)

Federal Energy Regulatory Commission (FERC)

International Boundary and Water Commission (IBWC)

Lower Colorado River Authority (LCRA)

National Oceanic and Atmospheric Administration (NOAA)

Natural Resources Conservation Service (NRCS)

State of Arkansas

State of California

State of California

State of Florida

State of Michigan

State of New Hampshire

State of New Hampshire

State of New Jersey

State of North Carolina

State of Pennsylvania

State of Pennsylvania

State of West Virginia

Tennessee Valley Authority (TVA)

U.S. Army Corps of Engineers (USACE)

U.S. Bureau of Reclamation (USBR)

U.S. Coast Guard (USCG)

U.S. Department of Energy (DOE)

U.S. Department of Homeland Security (DHS)

U.S. Department of Labor (DOL)

Levee Sub-Sector Coordinating Council

Within the Dams Sector, a Levee Sub-Sector Coordinating Council (LSCC) was established to lead efforts pertaining to the security and protection of levees and flood damage reduction systems. The LSCC currently consists of the following members:

Association of State Floodplain Managers (ASFPM)

Miami Conservancy District / NAFSMA

Factory Mutual Insurance Company (FM Global)

Los Angeles County Department of Public Works

Louisiana State Police

National Association of Flood and Storm Water Management Agencies (NAFSMA)

South Florida Water Management District

State of Arizona - Maricopa County

State of Louisiana - Southeastern Louisiana Flood Protection Authority – East (SLFPAE)

State of Louisiana - South La Fourche Levee District

United States Society on Dams (USSD)

Yazoo MS Delta Levee Board

Levee Sub-Sector Government Coordinating Council

In addition, a Levee Sub-Sector Government Coordinating Council (LGCC) was also established to serve as the counterpart and partner to the LSCC to develop, implement, coordinate, and execute protective programs and resilience-enhancing strategies relevant to levees and flood-risk reduction infrastructure systems across and between Federal Government agencies.

The LGCC currently consists of the following members:

U.S. Department of Homeland Security (DHS)

Federal Emergency Management Agency (FEMA)

International Boundary and Water Commission (IBWC)

State of California

U.S. Army Corps of Engineers (USACE)

National Resource Conservation Service (NRCS)

In addition to the Dams Sector Councils noted above, the DHS Cross Sector Cyber Security Working Group (CSCSWG) and the Industrial Controls System Joint Working Group (ICSJWG) provide further coordination on cyber-specific issues. In addition, the US-CERT, the Industrial Control System Cyber Emergency Response Team (ICS-CERT), and the Office of Cybersecurity and Communications, which are all also DHS organizations, provide cybersecurity information, along with the state-level organization, the Multi-State Information Sharing and Analysis Center (MS-ISAC).

Cross Sector Cyber Security Working Group

As with the SCCs and GCCs, the Cross Sector Cyber Security Working Group (CSCSWG) was established under the auspices of CIPAC to allow for government and private sector collaboration. This working group serves as a forum to bring the government and the private sector together to address cybersecurity risk across the critical infrastructure sectors. This cross-sector perspective facilitates the sharing of viewpoints and knowledge about various cybersecurity concerns, such as common vulnerabilities and protective measures, and leverages functional cyber expertise in a comprehensive forum. Managing cyber risk and securing cyberspace is an issue that cuts across the Nation’s critical infrastructure, and the cross-sector perspective ensures effective coordination with all of the sectors. Members of the Dams Sector Councils actively participate as members of the CSCSWG.

Industrial Control System Joint Working Group

The Industrial Control System Joint Working Group (ICSJWG) also operates under the auspices of CIPAC and was established in December 2008 to facilitate the collaboration of ICS stakeholders and to accelerate the design, development, and deployment of enhanced security for ICSs. ICSJWG participants include international stakeholders, government, academia, owner/operators, systems integrators, and the ICS vendor community. Their objective is to reduce the risk to cyber ICSs and coordinate across all critical infrastructure sectors, unlike this Roadmap that focuses exclusively on the Dams Sector. Members of the Dams Sector Councils also are active members of the ICSJWG.

United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) was established in 2003 and is a partnership between DHS and the public and private sectors that is designed to help secure the Nation’s Internet infrastructure and to coordinate defenses against and responses to cyberattacks across the Nation. The US-CERT provides a 24/7 single point of contact for cyberspace analysis and warning, information sharing, and incident response and recovery for a broad range of users, to include government, enterprises, small businesses, and home users. US-CERT is responsible for:

- Analyzing and reducing cyber threats and vulnerabilities;

- Disseminating cyber threat warning information; and
- Coordinating cyber incident response activities.

US-CERT also assists in the management, response, and handling of incidents, vulnerabilities, and mitigation of threat actions specific to critical control systems functions. A special section of US-CERT is devoted specifically to control system security, as described below.

Industrial Control System Cyber Emergency Response Team

The Industrial Control System Cyber Emergency Response Team (ICS-CERT) operates as a functional element of the US-CERT for cyber incidents related to ICSs. The ICS-CERT is responsible for analyzing and responding to cyber threats or issues affecting ICS security in critical infrastructure. DHS has recognized the need to expand upon these technical and response capabilities in order to improve situational awareness and incident response, and to minimize vulnerabilities. This expansion encourages government and private sector participation by reporting and sharing incident and vulnerability information.

Homeland Security Information Network – Critical Infrastructure

The DHS Homeland Security Information Network - Critical Infrastructure (HSIN-CI) is a Web-based system that provides situational awareness and facilitates information sharing and collaboration with public and private homeland security partners, domestically and internationally.

HSIN-CI is an important aspect of the Dams Sector information-sharing environment, as it provides a forum for its members to access sensitive but unclassified information relevant to a number of Sector issues. The HSIN-CI Dams Portal, managed by the Dams SSA within IP, provides trusted and vetted public and private sector partners, including owners and operators, with an effective Web-based tool with multiple capabilities and information-sharing components. The portal includes various communities of interest focused on specific activities and initiatives within the Sector; a reference library to provide information pertaining to issues such as security, protective measures, and crisis management; capabilities for suspicious activity reporting; and access to training modules.

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC)[1] is a collaborative organization with participation from all 50 States, the District of Columbia, local governments, and U.S. Territories. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cybersecurity readiness and response in each State and with local governments and territories. It provides a central resource for gathering information from the States on cyber threats to critical infrastructure and providing two-way sharing of information between and among the States and local government.

Operating under the auspices of MS-ISAC, the Local Government Cybersecurity Committee was established to help identify the cybersecurity challenges facing localities and to work toward solutions. This committee, which is voluntary and collaborative, is comprised of individuals representing towns, counties, cities, school boards, and a mix of State government representatives.

3. Challenges and Milestones

This chapter addresses the challenges associated with each of the control system security goals previously described in Chapter 2, which were developed to guide the efforts to improve the cybersecurity posture of the Dams Sector. In addition, corresponding milestones were established to address challenges and support the implementation of the control system security goals.

Challenges

Challenges to cybersecurity consist not only of the direct risk factors that increase the probability of a successful attack and the severity of the consequences, but also those factors that limit the ability to implement ideal security enhancements.

Risk is defined as the potential for an unwanted outcome resulting from an incident or event, as determined by its likelihood of occurrence and its associated consequences. The three components of risk are threat, vulnerability, and consequence. Threat is defined as a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Consequence is the effect of an event, incident, or occurrence.

The direct risk challenges include the threat (those who seek to attack and compromise a cyber system); the means of attack (which relies on taking advantage of system vulnerabilities); the nature of the system attacked (such as the age and configuration of the system); the value of the system; and how loss of control impacts the interaction with humans, property, and the environment.

Risk Challenges to Cybersecurity

- **Threat**
- **Means of attack**
- **Nature of system attacked**
- **Value of system attacked**
- **Interaction caused by loss of control**

Challenges related to the implementation of security measures include organizational, institutional, economic, and technical factors that either limit the availability of security measures or increase the difficulty of implementing optimum security enhancements.

One key technical challenge is the issue of accessibility, both physical and cyber, which could enable an attacker to take advantage of known and yet-to-be-discovered vulnerabilities. The accessibility issue is complicated by the global nature of the Internet and critical infrastructure. In this environment, an attack could originate from almost anywhere. One key business challenge companies have is the international nature of suppliers of cyber components and systems. Therefore, Dams Sector companies and agencies which own and operate ICSs need to be aware of the threat and vulnerability introduced by the international supply chain. This includes being aware of necessary updates to firmware and software. Risk assessment and analysis provides an analytical understanding of this problem. Systems and procedures should be designed and implemented in accordance with standards and accepted industry practices.

Goals and Milestones for Securing Control Systems

Given the challenges previously enumerated, various goals and milestones will be identified in this section that could potentially minimize or overcome those challenges. These goals and milestones often begin as a simple reversal of the challenge. For example, challenges—lack of knowledge, limited standards, limited capabilities, and need for a business case—lead to goals and milestones of enhancing training, improving standards, enhancing capabilities, and developing and using risk analysis, respectively.

GOAL 1 - MEASURE AND ASSESS SECURITY POSTURE

Companies and operational entities should have a thorough understanding of their current security architecture in order to determine control system vulnerabilities and actions that may be required to reduce them. Quantifying risk is a necessary component of risk assessment and subsequent resource allocation. This Roadmap presumes that the Dams Sector's owners and operators have the ability and resources to perform security monitoring of control system networks and to assess current security postures.

Goal 1

MEASURE AND ASSESS SECURITY POSTURE

Challenges

Understanding Risk

- Inventory of critical assets, their associated ICSs, and the risk of cyberattack are often not adequately known or understood.
- Knowledge and understanding of risk, including threat, vulnerability, defense, and consequence analysis capabilities across the Sector are limited.
- Cyber risk factors are neither widely understood nor accepted by technologists and managers.
- Practical and cost-efficient assessment tools are needed, but not widely available.
- Security vulnerability assessments are needed to determine the consequences of specific cybersecurity compromises of ICSs.
- The increasing number of ICS network nodes and access points has made identifying vulnerabilities more complex.
- A cyberattack on a vulnerable ICS could result in business interruption, loss of capital, and impacts to employees, public safety, the environment, and national security.

Measuring Risk – Metrics, Standards, Quantifications

- Cybersecurity threats are difficult if not impossible to quantify, but quantified values are required for quantified risk estimation.
- Security metrics are required to perform detailed threat analyses.
- Current standards for assessment of cyber vulnerabilities are inadequate.
- Existing standards lack meaningful and measurable specification relating to ICS cybersecurity.
- Consistent metrics to measure and assess security status are necessary, but unavailable.
- A risk assessment needs to be performed to help owners prioritize where investments need to be made.
- Metrics to measure cybersecurity posture and/or improvements over time and across the Sector are needed, but not available.

Physical Issues

- Physical and electronic isolation of many dam facilities increases the difficulty of assessing full threat and vulnerability parameters.

Milestones

Near Term (0-2 years)

- Integration of security into all operational plans
- Development of control system security recommended guidelines for use by the Dams Sector
- Development of common risk assessment metrics and standards
- Development of tools to assess security posture and compliance with pertinent regulations
- Dissemination of accepted ICS standards and guidelines that enable tools and metrics to be effectively deployed

Mid Term (2-5 years)

- Implementation of control system security recommended guidelines training programs throughout the Dams Sector
- Integration of control system security education, awareness, and outreach programs into Dams Sector operations
- Implementation of risk assessment tools throughout the Dams Sector — asset owners and operators begin performing self-assessments of their security postures
- Update Dams SSP as appropriate

Long Term (5-10 years)

- Development of continuous security monitors for dam control systems networks
- Perform active cybersecurity risk assessments of ICS security profiles, including benchmark comparisons against other sectors

GOAL 2 - DEVELOP AND INTEGRATE PROTECTIVE MEASURES

Companies and operational entities should develop and apply protective cybersecurity measures to reduce system vulnerabilities, system threats, and their consequences. Policy and technology solutions should be developed for new and existing systems on an ongoing basis to meet emerging needs. Protective measures on legacy systems include the application of best practices and security tools, procedures and patches for fixing known security flaws, training programs for staff at all levels, and retrofit security technologies that do not degrade system performance. Legacy systems should be replaced or considered for upgrade with next-generation control system components and architectures that offer built-in cybersecurity measures.

Challenges

Accessibility Issues (open environments, remote access, multiple access points)

- There is widespread and continuous connectivity of IT and ICS—generally with remote access by multiple parties or devices.
- Many ICSs have remote access points without appropriate or adequate access control.
- Many ICSs have been designed, built, and operated within unsecured communication environments.
- Existing ICSs have numerous access points, no password, shared passwords, use of default vendor accounts/passwords, and/or inadequate firewall implementation.
- Many ICSs operate using unauthenticated command and control data.
- Basic security features are not enabled on ICSs.
- The complexity of ICS increases with an increase in the number of nodes.
- The use of commercial off-the-shelf (COTS) products greatly increases the risk to an ICS.

Legacy Upgrade and Patch Management Issues

- The inability to perform patch management in a timely manner due to system unavailability in a 24/7 operating environment.
- Older operating platform (legacy and hybrid) systems may have little to no vendor support, thus limiting their ability to secure the system.
- Security upgrades to legacy ICS are difficult to retrofit, can be costly, and may degrade system performance.

Milestones

Near Term (0-2 years)

- Development of sector-specific NIST Cybersecurity Framework guidance
- Identification of existing risk management activities, tools, and solutions applicable to the Dams Sector within the NIST Cybersecurity Framework
- Development of control system protection guidelines for existing ICS
- Enabling existing ICS access controls
- Development and implementation of security patches for legacy systems
- Establishment of mechanisms to enhance information sharing between asset owners, operators, and vendors
- Identification and dissemination of best ICS security practices among owners and operators
- Development of guidance and education material associated with applicable project regulations
- Development of guidelines to secure or isolate ICS communications from public networks and communication infrastructures

Mid Term (2-5 years)

- Implementation of new protective tools and appropriate training
- Implementation of secure interfaces between ICSs and business systems where system isolation is not feasible
- Identification, publication, and dissemination of best practices, including ones for securing connectivity with business network and for providing physical and cybersecurity for remote facilities
- Development and implementation of high-performance, secure communications for legacy systems

Long Term (5-10 years)

- Secure integration of ICS and business systems where system isolation is not feasible

Goal 3 - Detect Intrusion and Implement Response Strategies

Cyber intrusions are becoming increasingly sophisticated, which is making it more difficult to protect ICSs from all cyber threats. Resilience requires that facilities have the ability to monitor system integrity, detect intrusions, and respond in a timely manner. Response requires the ability to detect and analyze anomalies and manage security events and response strategies aimed at increasing resilience.

Goal 3

DETECT INTRUSION AND IMPLEMENT RESPONSE STRATEGIES

Challenges

- Response activities can be hampered by asset owners' and operators' concerns regarding sharing of proprietary information (regarding past security events and their consequences) beyond the company.
- It is difficult to keep up with the continuously increasing sophistication and availability of hacker's tools and resources.
- Owners/operators failing to regularly review security logs results in limited response capability during emergencies, even when appropriate security measures are available.
- It is difficult to detect malware that is embedded in ICS hardware and is normally dormant until activated.

Milestones

Near Term (0-2 years)

- Leverage development of accepted industry practices on control system architecture and cybersecurity protection
- Integration of cyber incident response plans and procedures into emergency plans
- Identification and implementation of current security features built into control systems
- Development of best practices and guidelines for incident response and reporting
- Development of partnerships between asset owner/operators and vendors for Sector use of intrusion detection software
- Timely dissemination of control system risk information to Dams Sector partners

Mid Term (2-5 years)

- Implementation of intrusion detection software for monitoring Sector ICS
- Publication of related cybersecurity best practices and related training
- Implementation of training programs for intrusion detection software and any associated updates to response, identification, and reporting procedures
- Development of training for control room operators in identifying, reporting, and responding to unusual events, breaches, and anomalies caused by a cyber event
- Implement configuration management procedures and test beds for patch installations
- Development of public communication strategies for the dissemination of public safety training literature on the consequences of a disruption caused by a cyber event

Long Term (5-10 years)

- Implementation of real-time intrusion detection and prevention strategies within ICS networks
- Development of control systems security certification program for operators

GOAL 4 - SUSTAIN SECURITY IMPROVEMENTS

This goal focuses on sustaining the progress made in improving the protection and response capability of asset owners and operators. Maintaining aggressive and proactive cybersecurity of ICSs over the long term will require a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders. Over the next 10 years, Dams Sector owners and operators will collaborate within the Sector, across sectors, and with government to remove barriers to progress and create policies that accelerate sustained advancement in securing their ICSs.

Goal 4

SUSTAIN SECURITY IMPROVEMENTS

Challenges

Information Sharing Issues

- Information sharing lacks necessary and constructive relationships with governmental authorities for sharing Sector threat information.
- Cybersecurity is often handled separately from more traditional company security and safety programs.
- Federal legislative efforts to enhance national cybersecurity guidelines for Dams Sector facilities that proceed with limited input from owner/operators will likely create implementation problems.
- Establishing effective security-oriented partnerships between government and industry can be difficult.
- Inadequate and insufficient sharing of cyber threat and incident information between government and owners/operators negatively affects the ability to properly assess risk and select appropriate cybersecurity measures.
- The collaboration barriers between IT and ICS departments can lead to inconsistent and redundant security measures.

Investment Barriers

- Differing business models and risk profiles within the same operational boundaries (not all parts of a given multi-purpose dam or organization have the same potential for severe consequences) increase the difficulty and the number of incentives required to implement cybersecurity measures.
- Funding of activities (e.g. R&D) important to ICS security depends on input from industry to align government and industry goals.
- A cybersecurity business case based on enhanced risk analyses, which could quantify and prioritize necessary and sufficient security measures and justify the costs, is required, but not available.
- Funding and implementation of enhanced security measures is difficult without executive recognition of ICS security threats and liabilities.

Standards, Policies, and Cultural Practices Issues

- Consistent standards, requirements, and guidance applicable to the Sector are limited or lacking
- ICS cybersecurity across the many types of production facilities within the Sector is currently not always based on industry-accepted practices
- There are inadequate policies, procedures, and culture relating to ICS cybersecurity
- Periodic review of security logs and change management documentation often receives limited attention
- New regulations may impose requirements beyond the functional capability of legacy systems

Other Issues

- Implementing cybersecurity across the entire Sector is difficult due to varying needs of owners and operators and the large number of different assets within the Sector.
- Discovery of vulnerabilities, improved awareness, implementation of protective measures, and application of continuous improvement relative to cybersecurity are necessary to stay ahead of potential cyberattacks.

Milestones

Near Term (0-2 years)

- Widespread security awareness among Sector, cross-sector, government, and industry partners, and the general public with buy-in from key stakeholders, investors, and the public
- Development of mechanisms and guidelines for securely sharing accepted industry practices among Sector and industry partners
- Dissemination of industry-wide standards and best practices regarding ICS security tools, procedures, and training (assessment, protection, response) across the Sector

Mid Term (2-5 years)

- Development of government incentives for accelerated investment in cybersecurity measures
- Completion of cost-benefit analyses to determine business cases for voluntary cybersecurity investment
- Establishment of a life cycle investment framework for cybersecurity that can be tailored to the Dams Sector
- Formation of government/industry partnerships and designation of roles to help sustain best practices in industry

Long Term (5-10 years)

- Proliferation of training courses on cybersecurity and ICS protection
- Implementation of best cybersecurity practices to include performing regular upgrades and monitoring new threats across the Dams Sector

GOAL 5 - SECURE-BY-DESIGN

This goal is also concerned with sustainability and continuous improvement and focuses on the improvement and development of control system technology and tools that vendors develop, rather than the protection and response capabilities of owners and operators. Next-generation control system architectures should incorporate components that are inherently secure and offer enhanced functionality and performance. Control system designers should have security in mind when they are developing and/or customizing a product, or they risk potentially leaving "security vulnerabilities" within the product. Goal 5 anticipates that, within 10 years, ICS products that are secure-by-design with built-in end-to-end security incorporated into the lifecycle of ICSs will be available and used across the Dams Sector.

Goal 5

SECURE-BY-DESIGN

Challenges

- The increased use of standardized ICS technology and posture increases attack opportunity.
- Enhanced cybersecurity upgrades on ICSs with long-tern design capability that were not initially designed for current cybersecurity requirements may be difficult to upgrade and not cost efficient.
- Security that is not necessarily integrated into a vendor's ICS products increases inherent vulnerabilities, requires retrofits and upgrades, and still results in a less secure system.
- Poorly designed interconnections between ICSs and business networks can dramatically increase vulnerabilities and attack opportunities.
- Standardized security test plans and upgrades for all new-technology systems and components are not widely available, if at all.
- Tools and techniques sufficient to quantify or measure risk do not exist.
- Vendors do not have adequate requirements for standards to design and build cybersecurity into ICSs.
- Tested and validated cybersecurity tools for ICSs are lacking.
- There is a lack of incentives for vendors to implement and sustain secure-by-design enhancements to their ICS products.

Milestones

Near Term (0-2 years)

- Development of partnerships and increased collaboration between asset owners and operators and vendors
- Integration of control system security requirements into vendor contracts
- Utilization of procurement language developed by DHS for control systems
- Utilization of cybersecurity self-evaluation tool on a predetermined timeframe to measure Security Assurance Levels (SAL) of control systems

Mid Term (2-5 years)

- Establish lifecycle investment and framework for cybersecurity
- Partner and collaborate with government threat agencies (such as US-CERT, intelligence agencies, etc.)

Long Term (5-10 years)

- Commercial availability of next generation ICS architecture and components with built-in security that accommodate and anticipate changes in cyber threats and vulnerabilities
- Leverage existing available IT to develop as part of the control system, real-time security state monitoring capability that periodically tests and verifies that the required security functions are present and functioning

4. ROADMAP IMPLEMENTATION

This Roadmap contains a structured set of milestones that address specific ICS needs over the next 10 years. Achieving the goals' short-, mid-, and long-term milestones requires extensive information sharing at multiple levels; cybersecurity risk assessments that encompass threat, vulnerability, and consequences; cybersecurity business cases based on those risk assessments; engagement with control system vendors and the research and development community; and development of guidance documents and training materials.

The Dams Sector will pursue a focused, coordinated approach which aligns current activities to Roadmap goals and milestones; initiates specific projects to address critical gaps; and provides a mechanism for collaboration, project management, oversight, and information sharing among the Sector stakeholders. The objective of this approach is to accomplish clearly defined activities, projects, and initiatives that contain time-based deliverables tied to Roadmap goals and milestones.

Owners and operators are responsible for the security of their facilities and, therefore, must initiate business-critical projects that will ensure reliable, secure operation of dam facilities and assets. If owners and operators demand secure, reliable, and cost efficient systems and components, vendors will find ways to provide them.

Continuous improvements in securing control systems will be driven by ongoing information sharing and coordination efforts focused on the identification and development of efficient solutions in an environment consisting of multiple governing and regulatory agencies, independent facilities, and a variety of vendors and R&D organizations.

IMPLEMENTATION CHALLENGES

The security enhancement elements laid out by this Roadmap are voluntary and specifically avoid calling for regulation that would impose these priorities and actions on owners, operators, and vendors.

As a result of continuing cyberattacks against critical infrastructure, it is envisioned that ICS security enhancements will be incorporated into the life cycle of the systems. This will be based on each organization's understanding of the cost-benefit analysis of implementing security enhancements to reduce the risk of attack.

The difficulty in developing a cost-benefit analysis arises from the evolutionary nature of cyber systems and the fact that there is no long-term experience to project valid attack rate estimates. Quantifying the types of significant critical infrastructure attacks is also a challenge since the feared attack is expected to be an extremely rare event with extensive high impact costs. The difficulty in estimating the probability and consequence parameters to arrive at an economic risk (expected loss) is further exacerbated by the technical complexity of integrated cyber control system information. The milestones for Goal 1 were selected to enhance understanding of the need for system evaluations, risk assessments, and analyses that could ultimately result in a reliable cost-benefit analysis that would resolve the challenge and justify voluntary investment in necessary cybersecurity enhancement.

The challenge is to find a way to implement a voluntary effort aggressively and productively. The goals have been identified, in part, to help successfully implement this Roadmap. They begin with awareness, risk analysis, and self-assessment, and strive for long-term, cost-efficient technical solutions developed and provided by cyber ICS vendors.

In addition, the risk management planning process must include constant exploration of emerging ICS security capabilities, vulnerabilities, consequences, and threats to help sustain the collective stakeholders' efforts of developing this Roadmap.

This Roadmap encourages organizations to participate in ways that will best capitalize on their distinct skills, capabilities, and resources, for improving the security of ICSs. This affords companies and organizations the flexibility to pursue projects that correspond to their special interests.

Outreach, Training, and Education Needs

Within the Dams Sector, outreach, training, and education tools are critical in achieving a greater understanding of the potential impacts and consequences associated with cyber events. It is essential that the Sector enhance its awareness and understanding of these consequences in order to improve its ability to recognize cyber incidents when they occur and to respond to them effectively using the most reliable forms of mitigation available.

Dams Sector Council members have developed a strong partnership to help promote and facilitate Sector and cross-sector planning, coordination, collaboration, and information sharing for the protection of assets within the Sector. In continuing this cooperative relationship, the Sector should examine its current needs and shortcomings with regards to outreach, training, and education requirements.

The Dams Sector Security Education Workgroup, which consists of members from the Dams Sector Councils, has developed and distributed a multitude of reference documents focused on providing owners and operators with useful information regarding security awareness, protective measures, crisis management, and other security and protection related issues. These efforts represent the cornerstone of a successful outreach strategy intended to increase awareness and technical understanding across the entire Sector. The goal is to reach as many owners and operators as possible, regardless of the size or ownership of the facility.

Members of the Dams Sector Council, through the Security Education Workgroup, will continue to identify outreach, training, and education requirements in order to assist in achieving and sustaining the level of expertise needed to thwart cyberattacks on the Dams Sector ICS.

Information Sharing

Effective information sharing and awareness efforts help ensure the successful coordination and implementation of programs related to the protection of cyber assets, systems, networks, and functions. These efforts also enable cybersecurity partners to make informed decisions with regard to short- and long-term cybersecurity posture, risk mitigation, and operational continuity.

Utilizing effective methods for sharing information is critical in ensuring Sector partners have the capability to receive information that may enhance the protection of ICSs.

The Roadmap is an excellent example of a mechanism with which to conduct outreach and share information. It is intended to increase the Sector's situational awareness and offer suggestions focused on the reduction of potential consequences associated with cyber threats to ICSs.

Implementation Framework

Figure 3 illustrates the proposed implementation process for this Roadmap. The figure depicts the implementation carried out over three phases with an ongoing assessment of results and impacts feeding back into the implementation activities.

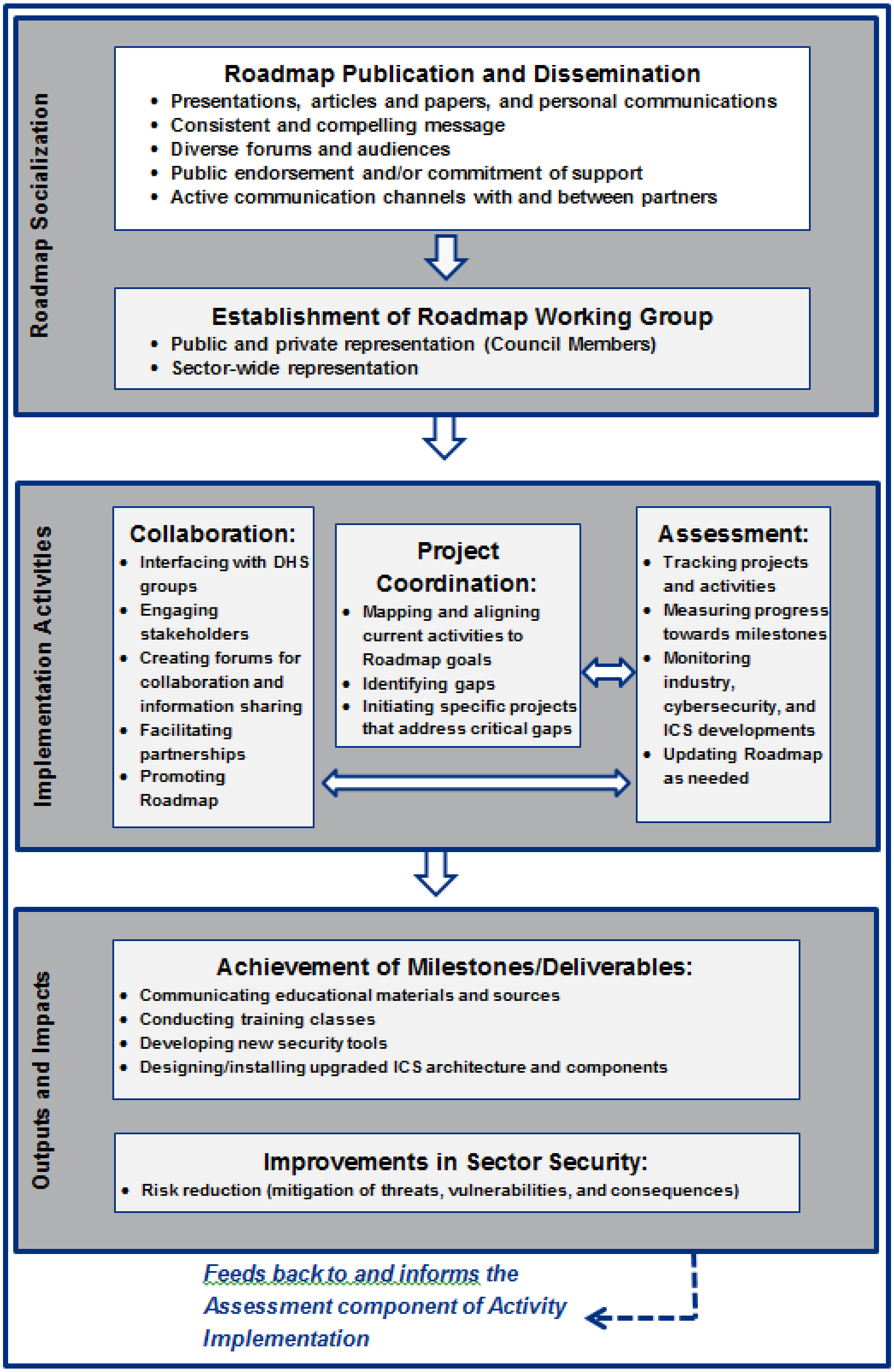

Roadmap Socialization
Roadmap Publication and Dissemination
• Presentations, articles and papers, and personal communications
• Consistent and compelling message
• Diverse forums and audiences
• Public endorsement and/or commitment of support
• Active communication channels with and between partners
Establishment of Roadmap Working Group
• Public and private representation (Council Members)
• Sector-wide representation
Implementation Activities
Collaboration:
• Interfacing with DHS groups
• Engaging stakeholders
• Creating forums for collaboration and information sharing
• Facilitating partnerships
• Promoting Roadmap
Project Coordination:
• Mapping and aligning current activities to Roadmap goals
• Identifying gaps
• Initiating specific projects that address critical gaps
Assessment:
• Tracking projects and activities
• Measuring progress towards milestones
• Monitoring industry, cybersecurity, and ICS developments
• Updating Roadmap as needed
Outputs and Impacts
Achievement of Milestones/Deliverables:
• Communicating educational materials and sources
• Conducting training classes
• Developing new security tools
• Designing/installing upgraded ICS architecture and components
Improvements in Sector Security:
• Risk reduction (mitigation of threats, vulnerabilities, and consequences)
Feeds back to and informs the Assessment component of Activity Implementation

Figure 3. Roadmap Implementation Process

Socialization

The first phase of the Roadmap implementation begins with the socialization process which involves the publication, dissemination, and promotion of the Roadmap among stakeholders. The experience of other sectors indicates that this is an important first step that builds support and buy-in, and lays the groundwork for the collaboration and partnerships required by the milestones. As the socialization efforts proceed, the Sector must be proactive in enhancing existing partnerships and forming new ones, as well as in identifying roles and delegating responsibilities. Then is the time to leverage buy-in from key players and to motivate industry leaders to step forward and become more actively involved. A critical component of the implementation process is the development of a roadmap workgroup (workgroup), which typically consists of members from the Dams Sector Councils and may include representatives from multiple stakeholder groups. The lessons learned from other sectors indicate that this workgroup should be formed early on and is vital to sustaining the momentum from the socialization process.

Implementation Activities

The second phase of the Roadmap is where the majority of the milestones, including policy development, partnership formation, training initiatives, and R&D efforts are implemented. The workgroup will serve as the mechanism for the project coordination of Roadmap activities and will take the lead in carrying out ongoing implementation activities in three areas: collaboration, project coordination, and Roadmap assessment.

Collaboration

The workgroup will provide venues for collaboration efforts; ensure the tools being developed enable the secure sharing of information (such as a shared portal for monitoring activities); and promote ongoing information exchange on best practices, industry developments, etc. The workgroup may also help further define the roles and responsibilities of Dams Sector stakeholders.

Project Coordination

The workgroup will take on a leadership role as project coordinator for Roadmap activities by assisting in defining roles and identifying, initiating, and tracking projects. One of the first steps will be to map current activities to Roadmap milestones and goals, identify gaps, and initiate specific activities that fill the gaps. The workgroup will help delegate tasks and subsequently track their progress over time in meeting Roadmap milestones.

Assessment

Project assessment involves the assessment and feedback of roadmap activities and ensures that they remain on target. In addition, it entails the assessment of industry developments in ICSs, IT, and evolving security threats that may affect Roadmap activities and require the readjustment of goals, milestones, and activities. As the workgroup tracks these changes, it may call for a revision to the Roadmap if the developments are significant.

The range of industrial control systems used in the Dams Sector and the range of their uses, coupled with evolving cyber-threats, complicates determining if satisfactory progress is being made in meeting the milestones outlined in the Roadmap. Therefore, annual summits of experts in industrial control systems, information technology, operations, and security could be convened to provide this assessment of progress across the Sector.

Outputs and Impacts

In phase three, properly managed and coordinated activities should lead to the creation of deliverables such as educational materials, documentation of best practices, Websites for information sharing, new security patches and tools, and upgraded ICS architecture and components. The concrete outputs and deliverables generated from the roadmap activities are deployed, primarily by owners and operators, and result in tangible improvements in cybersecurity of Sector assets. This accomplishes the mid- and long-term milestones and ultimately achieves the Roadmap goals.

AN ONGOING PROCESS

Initially, implementation is a sequential process whereby these phases occur consecutively. Over time, however, the implementation must transition to an ongoing process that usually includes revisions to both the goals and milestones. Ultimately, the Roadmap implementation becomes indistinguishable from the Sector's ongoing critical infrastructure security and resilience efforts. The Roadmap will provide its greatest value when it serves as an instrument of collaboration and a focal point for action within the Sector's overall security efforts.

The Roadmap will continue to evolve as industry reacts to business pressures, cyber threats, operational constraints, societal demands, and unanticipated events. While it does not cover all pathways to the future, implementation of effective programs to achieve the goals and vision identified in the Roadmap provides focus on what the Sector believes to be a sound approach to address the most significant ICS challenges within the next ten years including:

- A sector-specific baseline ICS security posture
- An effective communications and outreach strategy
- Training
- A self-certification program

As such, it is intended to guide the planning and implementation of collaborative cybersecurity programs which will involve owners and operators, industry associations, government, commercial entities, and researchers participating in the national effort to improve ICS security in the Dams Sector.

ROLES AND RESPONSIBILITIES

The responsibility for cybersecurity is shared by all critical infrastructure partners, including public and private entities, due to the interconnected nature of the cyber infrastructure. It is problematic to address the protection of physical and cyber assets independently since cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of critical infrastructure.

Several of the primary roles and responsibilities associated with various Sector partners related to the coordination, refinement, and execution of the overarching Dams Sector protective program are listed in the section below. The following list of responsibilities is not specifically associated with particular programs, projects, or funding; and does not constitute a commitment by a specific company, organization, or government agency:

- **DHS:**
    - Work with Dams Sector stakeholders to identify critical infrastructure security and resilience priorities for the Dams Sector
    - Provide information to help inform protective program decisions
    - Manage and facilitate the ICSJWG to coordinate deployment of Federal resources and minimize duplication of efforts
    - Support State, local, tribal, and private sector efforts by sharing threat information and issuing warnings.

- **Non-DHS Federal entities:**
  - Provide information to help make informed protective program decisions
  - Review security and resilience measures implemented by infrastructure owners and operators
  - Support international efforts to strengthen the security and resilience of critical infrastructure
- **State, local, tribal, and territorial governments:**
  - Supply the private sector with additional security and resilience guidance.
  - Provide National Guard, State, and local law enforcement personnel with other resources, as needed, in response to specific threat information and successful attacks
- **State government dam regulatory agencies:**
  - Work with USACE, Reclamation, and FERC, as appropriate, to ensure that State regulations relative to cybersecurity meet or exceed Federal standards and regulations
- **Sector owner/operators:**
  - Interact with DHS (US-CERT and ICS-CERT) to leverage available threat, incident, and vulnerability information
  - Implement site-specific security and resilience measures
  - Participate in identifying accepted industry practices
  - Report ICS, cyber incidents, or newly discovered vulnerabilities to the US-CERT at http://www.us-cert.gov/control_systems/
  - Share information within the Dams Sector and Federal agencies as required
- **Universities and colleges:**
  - Develop cyber ICS security courses
  - Establish cyber ICS security degree programs
  - Support the establishment and awarding of scholarships, fellowships, research assistantships, and other student financial support mechanisms
  - Support research and development activities

GUIDING AND ALIGNING EXISTING EFFORTS

As discussed in Section 2 and summarized in Table 1 below, a significant effort to enhance ICS security is already underway. These organizations and efforts provide a starting point from which to support the achievement of goals and milestones presented in this Roadmap.

Table 1. Selected control system security efforts.

Activity	Lead Organization	Scope	Major Actions and Events
Industrial Control System Joint Working Group (ICSJWG)	DHS Office of Infrastructure Protection and CIPAC	Coordinate Federal, State, and private sector initiatives to secure ICS	• ICSJWG quarterly and annual meetings.
Institute for Information Infrastructure Protection (I3P)	Dartmouth College, DHS Science and Technology Directorate, and NIST	National cybersecurity R&D coordination program	• I3P SCADA Security Research Project launched (2005) • I3P Research Report No. 1: *Process Control System Security Metrics* (2005) • *Securing Control Systems in the Oil and Gas Infrastructure, The I3P SCADA Security Research Project* (2005)
Control Systems Security Program	DHS Office of Cybersecurity and Communications, INL, and U.S. Computer Emergency Readiness Team (US-CERT)	Testing and Information Center for control systems cybersecurity	• Created and operates the ICS-Cyber Emergency Response Team (ICS-CERT) • Initiated the ICS Joint Working Group (ICSJWG) in December 2008 • Operates cyber vulnerability testing and assessment capabilities for installed control systems and vendor components • Develops risk analysis and self-assessment tools
ISA-99 Committee	ISA	The ISA-99 Committee addresses manufacturing and control systems whose compromise could result in any or all of the following situations: • Endangerment of public or employee safety • Loss of public confidence • Violation of regulatory requirements • Loss of proprietary or confidential information • Economic loss • Impact on national security	The committee has produced the following work products: • ANSI/ISA-TR99.00.01-2007, *Security Technologies for Manufacturing and Control Systems (2007)* • ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems: Concepts, Terminology, and Models* • ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program* The current emphasis is on addressing the topic "Technical Requirements for Industrial Automation and Control Systems." Working Group 4 will produce a series of standards and technical reports on this topic. The committee holds weekly working group meetings as well as general sessions at ISA EXPO (annually).
ISA Security Compliance Institute	ISA	Ensure that industrial control system products and services comply with industry standards and practices, "Development of test specifications and methodologies based on available standards and practices"	• ISA Security Compliance Institute Formal Launch – January 2008 • Certification Program Operations, Polices, and Processes Complete – November 2008

5. REFERENCES

1. Asenjo, Juan C., *Cybersecurity for Legacy SCADA Systems, Electric Light & Power*, September 1, 2005, (http://www.elp.com/index/display/article-display/237985/articles/utility-automation-engineering-td/volume-10/issue-6/features/cybersecurity-for-legacy-scada-systems.html).

2. Chemical Sector Roadmap Working Group, *Roadmap to Secure Control Systems in the Chemical Sector*, September 2009.

3. Federal Energy Regulatory Commission (FERC), FERC approves new reliability standards for cybersecurity, January 17, 2008 (http://www.ferc.gov/media/news-releases/2008/2008-1/01-17-08-E-2.asp).

4. Federal Energy Regulatory Commission, *Mandatory Reliability Standards for Critical Infrastructure*, Order No. 706, 2008 (http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf).

5. Florida Reliability Coordinating Council, *Reliability Standards Development Bulletin*, January 2008

6. Multi-State Information Sharing and Analysis Center (MS-ISAC), *About the MS-ISAC*, http://www.msisac.org/about/.

7. North America Electric Reliability Corporation, *Reliability Standards*, 2009, (http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx).

8. Northwest Hydroelectric Association, *Dam Safety and Security*, 2008

9. Shaw, William T., *SCADA Security: 14 Obvious Points of Attack, Electric Light & Power*, June 1, 2007, (http://www.elp.com/index/display/article-display/295755/articles/utility-automation-engineering-td/volume-12/issue-6/features/scada-security-14-obvious-points-of-attack.html).

10. Stamp, Jason, et al., *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia National Laboratory, May 22, 2003, (http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf).

11. Stouffer, Keith, et al., Revision 2 Final Public Draft, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology (NIST), Special Publication 800-82, February 2015. (http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf).

12. Turner, Aaron R., House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science & Technology - *Hearing on Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure*, Idaho National Laboratory, April 19, 2007.

13. U.S. Department of Homeland Security, *Dams Sector Security Awareness Guide - A Guide for Owners and Operators*, 2007, (http://www.damsafety.org/media/documents/DownloadableDocuments/DamsSectorSecurityAwarenessGuide_508.pdf).

14. U.S. Department of Homeland Security, *Dams Sector-Specific Plan*, 2015, (http://www.dhs.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf).

15. U.S. Department of Homeland Security, *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*, (https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf).

16. U.S. Department of Homeland Security, Written Statement of Donald (Andy) Purdy, Jr. Director (Acting), National Cybersecurity Division, July 19, 2005, (http://hsgac.senate.gov/public/_files/PurdyTestimony.pdf).

17. U.S. Department of Homeland Security, Control Systems Security Program (CSSP), (http://www.us-cert.gov/control_systems/).

18. U.S. Department of Homeland Security, Control Systems Security Program (CSSP), *Cyberthreat Source Descriptions*, (http://www.us-cert.gov/control_systems/csthreats.html).

19. U.S. Department of Homeland Security, Control Systems Security Program (CSSP), *Overview of Cyber Vulnerabilities*, (http://www.us-cert.gov/control_systems/csvuls.html).

20. U.S. Department of Homeland Security, Control Systems Security Program, Industrial Control Systems Joint Working Group (ICSJWG), (http://www.us-cert.gov/control_systems/icsjwg/).

21. U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team (US-CERT), US-CERT – About Us, (http://www.us-cert.gov/about-us).

22. U.S. Department of Energy, *Roadmap to Secure Control Systems in the Energy Sector*, January 2006 (http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf).

23. U.S. Government Accountability Office, *Critical Infrastructure Protection - Sector-Specific Plans' Coverage of Key Cybersecurity Elements Varies*, GAO 08-64T, October 31, 2007, (http://www.gao.gov/new.items/d0864t.pdf).

24. Water Sector Coordinating Council Cybersecurity Working Group, *Roadmap to Secure Control Systems in the Water Sector*, March 2008, (http://www.nawc.org/uploads/documents-and-publications/documents/document_4302bd61-e6fd-4a69-a73f-f4810ea7e5c0.pdf).

25. Weiss, Joseph M., *Control Systems Cybersecurity - The Need for Appropriate Regulations to Assure the Cybersecurity of the Electric Grid*, October 17, 2007, (http://realtimeacs.com/wp-content/downloads/pdfs/House-Hearing-10-17-Final.pdf).

6. ACRONYMS

ACL	Access Control List
AGA	American Gas Association
AGC	Automatic Generator Control
ASI	Advanced Systems Institute
ANL	Argonne National Laboratory
ANSI	American National Standards Institute
ASDSO	Association of State Dam Safety Officials
ASFPM	Association of State Floodplain Managers
AVC	Automatic Voltage Control
BCIT	British Columbia Institute of Technology
BES	Bulk Electric Systems
BPA	Bonneville Power Administration
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISSP	Certified Information Systems Security Professional
COTS	Commercial off-the-shelf
CREDA	Colorado River Energy Distributors Association
CPU	Central processing unit
CS	Control System
CS&C	Office of Cybersecurity and Communications
CSCSWG	Cross Sector Cybersecurity Working Group
CSSP	Control Systems Security Program
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DOL	U.S. Department of Labor
DSL	Digital Subscriber Line
EO	Executive Order
EPA	Environmental Protection Agency
ERO	Electric Reliability Organization

FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
GCC	Government Coordinating Council
GW	Gigawatt
HMI	Human Machine Interface
HSDRRS	Hurricane and Storm Damage Risk Reduction System
HSIN-CI	Homeland Security Information Sharing Network-Critical Infrastructure
HSPD-7	Homeland Security Presidential Directive – 7
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Computer Emergency Readiness Team
ICSJWG	Industrial Control System Joint Working Group
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
INL	Idaho National Laboratory
I/O	Input/output interface system
I3P	Institute for Information Infrastructure
IBWC	International Boundary and Water Commission
ICCP	Inter-Control Center Protocol
ICS	Industrial Control System
IP	Infrastructure Protection
ISA	International Society of Automation
IT	Information Technology
LAN	Local Area Network
LCRA	Lower Colorado River Authority
LFP	Local Flood Protection
LGCC	Levee Sub-Sector Government Coordinating Council
LSCC	Levee Sub-Sector Coordinating Council
MPLS	Multiprotocol Label Switching
MS-ISAC	Multi-State Information Sharing and Analysis Center
NAFSMA	National Association of Flood and Stormwater Agencies
NERC	North American Electric Reliability Corporation
NHA	National Hydropower Association
NIAC	National Infrastructure Advisory Council

NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NRCS	Natural Resources Conservation Service
NSC	National Security Council
NSF	National Science Foundation
NSTB	National SCADA Test Bed
OS	Operating System
PC	Personal Computer
PCS	Process Control System
PCSRF	Process Control Security Requirements Forum
PDA	Personal Digital Assistant
PLC	Programmable Logic Controller
PPD	Presidential Policy Directive
R&D	Research and Development
RTU	Remote Terminal Unit
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SLFPAE	Southeastern Louisiana Flood Protection Authority (East)
SONET	Synchronous Optical Network
SP	Special Publication
SSA	Sector-Specific Agency
SSP	Sector Specific Plan
TVA	Tennessee Valley Authority
USACE	United States Army Corps of Engineers
USBR	U.S. Bureau of Reclamation
USCG	United States Coast Guard
US-CERT	United States Computer Emergency Readiness Team
USSD	United States Society on Dams
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Local Area Network

Appendix A
Glossary: Definition of Terms

Disclaimer: The terms and definitions referenced in this glossary are specific to their use in this document. No attempt has been made to correlate the definitions of the terms in this glossary with similar terms in other documents or standards.

Term	Definition
Access Control List	An ACL is a list of security protections that applies to an object. An object can be a file, process, event, or anything else having a security descriptor.
Central Processing Unit	A CPU or processor is an electronic circuit that can execute computer programs.
Commercial Off-the-Shelf	COTS refers to commercially available technological components and systems, including both hardware, and software.
Control System	A CS is a device or group of devices that monitor, manage, command, direct or regulate the behavior of other devices or group of devices.
Distributed Control Systems	A DCS is a type of plant automation system similar to a SCADA system, except that a DCS is usually employed in factories and is located within a more confined area. It uses a high-speed communications medium, which is usually a separate wire (network) from the plant LAN. A significant amount of a closed loop control is present in the system.
Human-Machine Interface	A HMI are operator interface terminals or personal computers with which users interact in order to control other devices.
Industrial Control Systems	ICS is a general term that encompasses several types of control systems and, for the purpose of this Roadmap, it is defined as the facilities, systems, equipment, services, and diagnostics that provide the functional monitoring, control, and protection capabilities necessary for the effective and reliable operation.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the organization. The term information technology includes computers, ancillary equipment, software, firmware, similar procedures, services (including support services), and related resources.
Local Area Network	A LAN is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.
Personal Computer	A PC is a single-user system based on microprocessors.
Personal Digital Assistant	A PDA is a handheld device that combines computing, telephone/fax, Internet, and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser, and personal organizer.

Term	Definition
Process Control Systems	Descriptive of systems in which computers or intelligent electronic devices are used for automatic regulation of operations or processes. Typical operations are when the control is applied continuously and adjustments to regulate the operations are directed by the computer or device to keep the value of a controlled variable constant— contrasted with numerical control.
Programmable Logic Controllers	A PLC or programmable controller is a digital computer used for automation of electromechanical processes such as control of machinery in factories, power plants, manufacturing processing facilities, refineries, pipelines, etc.
Remote Terminal Unit	An RTU is a device installed at a remote location that collects data, codes the data into a format that is transmittable, and transmits the data back to a central station, or master control center.
Supervisory Control and Data Acquisition	A computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation.
Virtual Private Networks	A VPN is a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. Some of these systems use encryption and other security mechanisms to ensure that only authorized users can access the network, and that the data cannot be intercepted.
Wide Area Network	A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).
Wi-Fi	The name of a popular wireless networking technology that uses radio waves to provide high-speed Internet and network connections. Wi-Fi refers to any wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards

Appendix B
National Policy Guidance on Cyber Control System Security

The risk America faces from cyber applications is one of the most urgent national security problems facing the country. In the new global competition where economic strength and technological leadership are vital components of national power, failing to secure cyberspace puts the United States at a disadvantage. A White House official wrote on March 2, 2009, that "our Nation's security and economic prosperity depend on the security, stability, and integrity of communications and information infrastructure that are largely privately-owned and globally-operated."[c] Furthermore, the *National Strategy to Secure Cyberspace* (February 2003) states that "the cornerstone of America's cyberspace security strategy is and will remain a public-private partnership."

As early as 2009, the Annual Threat Assessment indicated that nation states and criminals were targeting government and private sector information networks within the United States to gain competitive advantage in the commercial sector.[d] A successful cyberattack against a major financial service provider could severely impact the national economy; while cyberattacks against physical infrastructure computer systems, such as those that control power grids or oil refineries, have the potential to disrupt services for hours or weeks. In a speech at Purdue University on July 16, 2008, while campaigning for President, Barack Obama said that

> *"Every American depends—directly or indirectly—on our system of information networks. They are increasingly the backbone of our economy and our infrastructure; our national security and our personal well-being. But it's no secret that terrorists could use our computer networks to deal us a crippling blow. We know that cyber-espionage and common crime is already on the rise. We need to build the capacity to identify, isolate, and respond to any cyber-attack."* [e]

The Center for Strategic and International Studies report on cybersecurity for the 44th Presidency concluded that (A) cybersecurity is now a major national security problem for the United States, (B) decisions and actions must respect privacy and civil liberties, and (C) only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure. The report continues by stating that the United States faces "a long-term challenge in cyberspace from foreign intelligence agencies and militaries, criminals, and others—that losing this struggle will wreak serious damage on the economic health and national security of the United States." [f]

The Nation has responded to this threat through the following directive and laws:

[c] John Brennan, Assistant to the President for Homeland Security and Counterterrorism, http://www.whitehouse.gov/blog/09/03/02/Cyber-review-underway/ (Accessed 1/20/2016)

[d] Dennis C. Blair, Director of National Intelligence, 12 February 2009, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* *http://www.dni.gov/files/documents/Newsroom/Testimonies/20090212_testimony.pdf* (Accessed 1/20/2016)

[e] http://www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.html (Accessed 1/20/2016)

[f] U.S. Senate, March 2009, Cybersec.4, Staff Working Draft, http://cdt.org/security/CYBERSEC4.pdf (Accessed 1/20/2016)

- In 1988 Presidential Decision Directive NSC-63 (PDD-63), “Critical Infrastructure Protection,” was issued recognizing the need for enhanced security of the Nation’s cyber aspects of critical infrastructure. Although directed specifically to information systems, it recognized the interdependencies within the critical infrastructure sectors and the reliance of that infrastructure on automated cyber systems. The directive called for voluntary private-public partnerships of the type formalized in the National Infrastructure Protection Plan (NIPP), provided an assignment of government agencies as lead sector agencies, and called for the creation of a private sector information sharing and analysis center which evolved into the Sector Information Systems Advisory Councils.

- The Federal Information Security Management Act of 2002 (FISMA) requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the Government Facilities Sector-Specific Plan.

- The *Cybersecurity Research and Development Act of 2002* allocates funding to the National Institute of Standards and Technology and the National Science Foundation for the purpose of facilitating increased research and development (R&D) for computer network security and supporting research fellowships and training. The act establishes a means of enhancing basic R&D related to improving the cybersecurity of critical infrastructure.

- The *National Strategy for Homeland Security* and the *Homeland Security Act of 2002* responded to the attacks of 9/11 by creating the policy framework for addressing homeland security needs and restructuring government activities, which resulted in the creation of the Department of Homeland Security (DHS).

- In early 2003, the *National Strategy to Secure Cyberspace* outlined priorities for protecting against cyber threats and the damage they can cause. It called for DHS and DOE to work in partnership with industry to “... develop accepted industry practices and new technology to increase security of DCS/SCADA, to determine the most critical DCS/SCADA-related sites, and to develop a prioritized plan for short-term cybersecurity improvements at those sites.”

- In late 2003, the President issued Homeland Security Presidential Decision 7 (HSPD-7), “Critical Infrastructure Identification, Prioritization, and Protection,” to implement Federal policies. HSPD-7 outlined how government will coordinate critical infrastructure protection and assigned DHS the task of working with the Dams Sector to improve physical and cybersecurity of the Dams Sector. Responsibilities include collaborating with all government agencies and the private sector, facilitating vulnerability assessments of the Sector, and encouraging risk management strategies to protect against and mitigate the effects of attacks. HSPD-7 also called for a national plan to implement critical infrastructure protection.

- Executive Order 13231 (as amended by E.O. 13286 of February 28, 2003 and E.O. 13385 of September 29, 2005) established the National Infrastructure Advisory Council (NIAC) as the President’s principal advisory panel on critical infrastructure protection issues spanning all sectors. The NIAC is composed of not more than 30 members who are appointed by the President and selected from the private sector, academia, and State and local governments. They represent senior executive leadership expertise from critical infrastructure areas as delineated in HSPD-7. The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructure, both physical and cyber. The NIAC is charged with improving the cooperation and partnership between the public and private sectors in securing critical infrastructure, and advising on policies and strategies that range from risk assessment and management, information sharing, and protective strategies to clarification of roles and responsibilities between public and private sectors.

- The *National Infrastructure Protection Plan* was issued in 2006 (Revised in 2009 and 2013). It establishes a partnership model for collaboration that consists of a Sector Coordinating Council and a Government Coordinating Council for each sector in accordance with the laws, directives, and strategies described above. The SSA for the Dams Sector is the Office of Infrastructure Protection within DHS.

Within the Dams Sector, the Dams Sector Coordinating Council (SCC) serves as the private sector interface with the Federal Government on issues related to the security of dams, locks, and levees. Its primary purpose is to determine the nature of risks posed against Sector assets so that appropriate and timely information, as well as mitigation strategies, can be provided to the entities responsible for the operation and protection of those assets. The SCC also serves as the principal asset owner interface with other critical infrastructure sectors, as well as with DHS, the Federal Energy Regulatory Commission (FERC), and other government agencies, including the Dams Government Coordinating Council (GCC).

The Dams GCC acts as the government counterpart and partner to the SCC to plan, implement, and execute sector-wide security and resilience programs for the Sector's assets. It is comprised of representatives from various levels of government (Federal, State, local, and tribal), including Federal owners and operators and State and Federal regulators of Sector assets. Its primary activities include identifying issues that require public-private coordination and communication; bringing together diverse Federal and State interests to identify and develop collaborative strategies that advance critical infrastructure security and resilience; assessing needs and gaps in plans, programs, policies, procedures, and strategies; acknowledging and recognizing successful programs and practices; and leveraging complementary resources within government and between government and industry.

Member of the Dams Sector Councils collaborated with DHS to issue the 2007 *Dams Sector-Specific Pla*n *(SSP)* with a 2010 and 2015 update. The 2015 SSP specifically addresses the cyber needs of control systems in the Dams Sector.

The NIPP provides a more extensive descriptive listing of laws, directives, and guidance for critical infrastructure protection, which includes those pertaining to cybersecurity and other forms of risk.

Appendix C
Industrial Control System Details

IMPORTANCE OF INDUSTRIAL CONTROL SYSTEMS IN THE DAMS SECTOR

ICSs assist in the efficiency and safety of dam operations and missions. These systems provide the capability for remote control and monitoring of operations from a centralized control center through various modes of communication, technologies, and methods.

Dam operations are controlled either onsite or remotely and may rely to some extent on ICSs for operation or monitoring purposes. ICSs use transducers to collect information about dam operations and facilities, converting information (such as gate position, reservoir level, hydroelectric generator output, and water flow) to electrical signals to be processed by the ICS computers. When information falls outside expectations, alarms may be triggered to inform controllers and operations staff of the situation, enabling them to take corrective actions. Some ICSs may also automatically take some corrective actions without the interaction of the facility’s staff.

ICS designs and implementations vary from project to project due to the variety of projects and their specific requirements. A common solution may include a customized combination of COTS hardware and software, or it may include a proprietary system of hardware and software.

Dams, especially those located upstream of densely populated areas, may be considered high risk due to the potential for extreme consequences in the event of a catastrophic failure. However, if they do not have any technical components that would be considered vulnerable to a cyberattack, they may be high risk only from a physical standpoint. If the operation does not include significant control system functions, the cyber exposure may be minimal.

Cybersecurity plays a key role in the operation and maintenance of some of these complex systems, particularly with those systems where security measures were not included in the original design.

INDUSTRIAL CONTROL SYSTEMS

Industrial Control Systems (ICS) is a general term that encompasses a wide variety of control systems. Typically, in a power generation project such as a hydropower plant, the ICS is also known as a Supervisory Control And Data Acquisition (SCADA) system. The term SCADA usually refers to centralized systems that monitor and control entire sites, or complexes of systems spread out over large areas. The monitoring aspects of a SCADA system are normally done through sensors throughout the system collecting the needed data. Most control actions are performed automatically by remote terminal units (RTUs) or programmable logic controllers (PLCs).

Another common term used in the Dams Sector when talking about ICS is distributed control systems (DCS). A DCS refers to a control system in which the controller elements are not central in location, but are distributed throughout the system with each component subsystem controlled by one or more controllers. The entire system of controllers is connected by networks for communication and monitoring. In addition, elements of a DCS may directly connect to physical equipment such as relay switches, pumps, and valves, or may work through an intermediate system such as a SCADA system.

A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world with a DCS or SCADA system by transmitting telemetry data between those objects and the system. PLCs are ruggedized microcomputers with hardware and software specifically designed to perform industrial control operations. A PLC consists of two basic sections**:** The central processing unit (CPU), and the input/output (I/O) interface system**.** An RTU unit differs from a PLC in that RTUs are more suitable for wide geographical telemetry, often using wireless communications, while PLCs are more suitable for local area control where the system utilizes physical media for control.

Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status reports that are communicated to a SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the Human Machine Interface (HMI) can make supervisory decisions to adjust or override normal RTU or PLC controls. Data may also be fed to a Historian, often built on a commodity Database Management System, to allow trending and other analytical auditing.

Host control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the generation unit based on the flowrate of water through part of a hydropower production process and the current power demand; however, the SCADA (ICS) system may allow operators to change the set points for flowrate and enable alarm conditions (e.g., loss of flow and high temperature) to be displayed and recorded. The feedback control loop passes through the RTU or PLC, while the SCADA system monitors the overall performance of the loop.

Automated dam performance monitoring systems, which include local wireless data acquisition networks, can provide automated real-time data collection and analysis of inflow, outflow, gate position, and water surface elevation.

Existing ICSs in the Dams Sector vary widely based on the age and generation of the systems; thus, they also vary with respect to complexity and sophistication. Some ICSs are closed and use isolated networks as well as proprietary communications protocols. Other ICSs are open and use open architectures, common communications paths, and rely on the Internet. In addition, cyber systems at dams may also be connected to the electrical power grid. Most, if not all, dam owners use various computer security methods on master terminal units, data servers, and historians. These security methods include authentication procedures, encryption, firewalls, anti-virus software, and anti-spyware software.

In general, ICS complexities depend on a variety of factors, including the age and generation of the system. Typically, the larger the project's geographical footprint, the more sophisticated the ICS becomes. Furthermore, a highly automated system with much built-in redundancy tends to be more elaborate.

In smaller projects, such as a single function facility, the typical ICS is simpler. For example, in a project whose function is only to supply water, local operator consoles, rather than a formal control center, are relied upon to monitor and control the system.

ICSs for water supply systems are used to control and monitor remote operations of penstock and spillway gates, to control water levels in reservoirs, and to provide seasonal weather data using the common control system network. Due to the primary mission of meeting the water needs of the local population, a water supply facility is normally coupled tightly to the local water organization and its constituents. Due to this tight bond and the need of the community to interact with the water supply, the ICSs are normally more open, which in turn, increases their vulnerability to outside attacks.

Risk to control systems in terms of reliability may increase as physical surveillance systems are being piggybacked off of the same ICS communication networks and bandwidth. To help mitigate the risk of an attack, the ICS should be isolated from other systems by using a one-way link to push data. For example, the link could be implemented by using a passive file transfer solution where data is placed in one part of a network that is connected to an outside network through a one-way link.

In other cases, the ICS may be connected to a Web-based service that gives consumers the ability to directly interact with the ICS by supplying orders of quantity of water and searching for information about the quality and quantity of water delivered. The communication network for water supply ICS could be common for other business and weather monitoring systems (e.g., use of public telephone network such as T1, partial T1, DSL, etc.). As previously stated, risk to control systems, in terms of reliability, may increase as physical surveillance systems are being piggybacked off of the same ICS communication networks and bandwidth. ICS are also used to obtain data from sensors reporting water quality issues, dissolved gases in water, fish habitat, and control of water flow. Although this may improve the level of interaction between the facility and its constituents, it opens up the ICS to the outside world. Protective measures to help mitigate the risks associated with this scenario include the use of properly configured firewalls, data encryption, separation of internal networks between control and communication, or a combination of these.

ICSs are used to control and monitor electrical generating equipment. ICSs of power generation facilities are normally more sophisticated than those of water supply facilities. For example, power generation control systems are used to control governors and governor systems, relays, voltages, frequencies, and automatic voltage regulators among others. In the future, there will be more pressure to provide power system stabilizer information from governor systems. This could lead to increased vulnerability of power systems.

Control operations at a hydropower generation plant can be managed through a DCS with data acquisition. The ICS interfaces with a control center, which monitors and controls hydropower generation via Ethernet. These systems frequently use an unencrypted backbone infrastructure as a gateway to the DCS which connects with RTUs.

ICS are available through a wide variety of network architectures, including COTS, HMI, data acquisition and control, and monitoring software and hardware. In addition, ICSs with proprietary protocols and codes can also be developed and used for specific projects. Usually, ICSs use extensively modified versions of the Microsoft Windows operating system to monitor the performance and operation of hydropower generation using RTUs interconnected to the power generation local DCS. The systems are designed to operate in a closed loop network with alternative hard-wired controls for start/stop, as well as data monitoring of the power turbines and generation equipment, as a backup. The systems may also have the ability to be interconnected with other networks, mainly through internet protocols (IP) or other communication standards.

Some hydropower operations employ ICSs using known vendor PLC units to operate hydropower generation plants on an Ethernet LAN from the control center. The power generation equipment uses a DCS connected to the above-mentioned ICSs. The Master Terminal Unit normally uses a Windows based operating system and a COTS HMI interface. The power generation DCS uses RS232 serial data protocol.

In some cases, power generation projects use separate hard-wired systems as a backup, using Automatic Generator Control (AGC) prior to going to full manual control of generation equipment by field personnel. The disruption of any command and control signal to devices in the power generation plant does not impact its operation because the PLCs continue to operate at the last field device setting. Hard-wired backup systems usually do not include external links to other networks, and all hardware, software, communication equipment, and Ethernet local area networks are within the physical security perimeter of the project.

An additional system (widely used throughout projects) is Automatic Voltage Control (AVC), which heightens system efficiency and power quality by automatically monitoring and controlling busbars, transformers, and tertiary reactors. On a power distribution system experiencing varying loading conditions, this sophisticated substation automation application can effectively maintain a steady transformer secondary voltage within preset limits.

Hydropower generation projects must, by law, report to the corresponding regional transmission organization (RTO). In the United States, an RTO is an organization that is responsible for moving electricity over large geographical areas by coordinating, controlling, and monitoring a large electricity transmission grid. For projects with this requirement, ICSs may have a direct communication link to the RTO control center. This communication link can be created via microwave, as well as through secure lines using an inter-control center protocol (ICCP) for data, such as voltage, frequency, current, power, etc. This communication path can also be used by the RTO to send requirements to the project. The communication occurs through a dedicated data encrypted link. As a general rule, projects communicate with an RTO for any operational changes via data transmission over a public switched telephone network. The RTO does not have access to the controls of hydropower generation equipment and/or field devices. If an incident occurs that forces the project into manual operation, communication between the project and the RTO is conducted through a voice system.

Spillway gates are an essential dam component as they are used to control water releases from the reservoir to areas downstream of the facility. In some projects, the spillway gates are manually controlled with no infrastructure or communication existing between each gate or to any central controller system. In some projects, the spillway gates are controlled and monitored by an ICS that can either be directly connected or completely separate from other ICSs in the project. In the case where spillway gates are controlled by an ICS, the manual controls are normally used as backup control in the event of ICS failure.

Some projects that are required to monitor and control operations within a wide geographical area use leased partial dial-up modem connections over the Public Switched Telephone Network, or dedicated T1 lines, depending on the flow of data. Similarly to communication between the ICS and the RTO, this communication may include the use of firewalls and encryption of data for security purposes. Additional modes of communication may also include the use of wireless systems, such as a microwave signal, or the use of specialize networks, such as the Synchronous Optical Network (SONET), Multiprotocol Label Switching (MPLS), Optical Ethernet, etc. In some cases, to save the cost and time of designing and implementing separate communication networks, communication links for the ICS, administrative networks, and other networks are bundled into the same backbone, thereby introducing a single point of failure into the system.

Some projects that remotely monitor and periodically control operations do not have AGC links to other projects since all remote functions are auto-synchronized at each project site. Each project site has local control panels for full project control as a backup mechanism.

Within some projects, the safety power relay switches are hardwired and connected to a network separate from that of the ICS, even though the systems may have the capability to interconnect. In other cases, ICSs include a direct connection to the networks that include power relay switch systems and other protection systems.

In some instances, hydropower, water control, and fish ladder monitoring and control systems are all connected to an ICS. Business systems and ICS networks are universally separate in the Dams Sector, except in some cases for the data historian, which provides a bridge or a link between the ICS and corporate information systems. The separation between the control system network and the other networks provides a higher level of protection for the project by lowering the number of access points and the number of direct and indirect connections. By lowering the number of access points to the control network, the flow of data traveling to and from the control network is better managed. In addition, by lowering or eliminating the number of interconnections between the control system network and other networks (e.g., business or security networks), the flow of data traveling between the two networks is more easily managed and less vulnerable to being intercepted by the outside world.

In some projects, maintenance of the ICS and/or its components is commonly outsourced to third party vendors. These vendors can access the ICSs using remote dial-in modems on a demand basis only. The process for on-demand requests usually involves the following steps:

1. Direct communication between the vendor and organization (i.e., phone, email) requesting vendor access to the system.
2. The project operator or assigned personnel physically connects the dial-up modem to the system.
3. The project operator or assigned personnel authorizes a temporary password to access the system.
4. Following completion of the work, the dial-up modem is physically disconnected from the system.

Navigation locks and dams are used to maintain water levels for the transportation of commercial goods and commodities. Many existing navigation locks use relay-based control systems; however, several navigation locks also use PLC systems which are becoming the preferred system. The control systems for navigation dams are similarly diverse.

Both relay-based systems and PLC systems, depending on the sophistication level and integration of the system, can control gates, open and close valves, lock signals, lock lights, and enable interlock safety control features as well as all of the lock's electrical and mechanical subsystems. The PLC system, which usually incorporates a backup control system, also provides monitoring and reporting of lock equipment status. Control of lock equipment is initiated by the onsite operators either from a control stand located adjacent to the equipment or from the navigation lock's central control station. Some PLC control systems may allow remote monitoring and control on secure systems.

Retrofitted Control Systems

Legacy systems are especially vulnerable to computing, communication system resource availability, and timing disruptions. Many systems do not have security features such as encryption capabilities, error logging, and password protection. For ICSs where technology has been developed for a very specific use, the lifetime of the deployed technology is often 15 to 20 years or longer. The useful life of a PLC is much longer than that of the operating system (OS) and the HMI software. Since some OSs today are open, patches and configuration management can cause problems and vulnerabilities. In many cases, security patches applied to new control systems may cause a legacy system to crash. There is always a distinct vulnerability due to technological incompatibility. Achieving a comfortable level of security requires non-intrusively retrofitting unsecure legacy ICSs with new technology. In most cases, it is not economically and technically feasible to retrofit security appliances to the existing control system infrastructure.

Improving the security of legacy ICSs against cyberattacks requires flexible solutions that are easy to install and which do not impact system performance or operations. Development of retrofit solutions that can provide robust cybersecurity to existing fielded ICSs has been of particular interest to industry organizations such as NERC, the Gas Technology Institute, and the International Society of Automation. Since ICSs are typically functional beyond 15 years, retrofit solutions are usually implemented to address cybersecurity concerns and to meet fielded systems compliance requirements, while embedded security features are designed as part of a more robust ICS in the future. The efforts of the aforementioned organizations are yielding security recommendations, including NERC CIP, and the American Gas Association (AGA-12) standard, which provide guidelines on the establishment of security policies and procedures, including the use of retrofit cryptographic devices. The need for increased interconnectivity, faster data transmittal, and older system connectivity to newer control systems are factors which increase the level of vulnerability and the probability of an incident occurring in an ICS.

Integrating new technologies into these systems is often difficult and occasionally impossible. For example, older versions of some operating systems may no longer be supported by the vendor, thereby making some OS patches useless. In some cases, the patches will simply interrupt communication lines between the equipment and shutdown the system. To reduce the probability of these types of events from occurring, some projects have created test beds replicating the ICS (in a private network) and have been able to view the effects patching without compromising the system. The test bed should include a policy that states a minimum amount of time for testing, in order to produce realistic results.

Many legacy systems have taken advantage of newer technologies and created electronic security perimeters to protect themselves, without having to invest in newer, more secure systems. Technologies presently available for the protection of ICSs include firewalls, honeypots, antiviral software, cryptography, intrusion detection and prevention systems, etc. With these technologies, the security of existing ICSs can be significantly enhanced to protect against cyberattacks.

The use of firewalls in the perimeters of ICSs prevents unwanted communication from reaching the equipment. Firewalls, if configured correctly, can effectively prevent an entity that may reside in the corporate network from taking over the control network, and vice versa. Honeypots, for example, generally consist of a network site that appears to contain information that would be of value to attackers; however, it actually serves as a trap, which is isolated and monitored, to detect, deflect, or, in some cases, counteract attempts at unauthorized entry to the system. The main objective of antivirus software is to prevent the attack and/or remove computer viruses, worms, Trojan horses, adware, spyware, and other malware.

Cryptography is the use of mathematical formulas and techniques to convert a comprehensible message into an incomprehensible message, and then back again, to prevent information from being easily understood if intercepted. Retrofit solutions of this type will protect communications throughout the system. Unique features necessary in the retrofit solutions include strong authentication and encryption for access control, as well as the protection of message integrity and confidentiality.

Deploying retrofit cryptographic solutions to address the critical data communication security needs of existing ICSs has come to be known as a “bump in the wire” solution. In some cases, the solutions can be installed without affecting the control system infrastructure already in place or disrupting the system’s performance. In other cases, the use of this technology will affect the software patch by delaying the flow of information and, in some cases, shutting down the complete system. To help prevent an event from occurring throughout the system, a phased-in approach should be utilized when implementing this type of solution, initially across the more vulnerable connections, followed by wider deployment across the entire ICS network.[g]

An Intrusion Detection System (IDS) represents a type of software, hardware, or a combination of both inside a network designed to detect and alert if malicious behaviors are occurring within the network. The three basic parts of the IDS include sensors to detect events, a console to monitor the system and produce relevant alerts, and a processor to record the events and create the alerts needed.

[g] Utility Automation & Engineering T&D, 2005, Cybersecurity for Legacy SCADA System, Asenjo, Juan C. http://www.elp.com/articles/powergrid_international/print/volume-10/issue-6/features/cybersecurity-for-legacy-scada-systems.html (Accessed 1/20/2016)

An Intrusion Prevention System is basically an IDS with the added feature of being able to react to the malicious behaviors by blocking and/or preventing further activities in the system.

Since most ICSs are designed on top of unsecure networks, security measures in the network layer should be implemented. Some of these measures include packet filtering, sniffing, and access control list (ACL). Packet filtering is a technique that looks at each packet of data entering or leaving the network and accepts or rejects the packet of data based on rules of communication defined by the owner or operator of the network. Packet sniffing, also known as packet analyzer, represents a product comprised of software, hardware, or a combination of both that intercepts and logs traffic within the network, and further decodes and analyzes the packet data. Finally, an ACL is a list of permissions that specifies what type of data can be accessed (and by whom), as well what operations are allowed to be performed on that data.

When using a combination of the above technologies, ICSs are completely separated from the power relay switch systems as well as from the communication systems; therefore, it becomes more difficult for an outsider attack to occur since it requires a coordinated attack involving multiple networks. Furthermore, in order for the outsider to be able to take over the ICS, the attacker must enter through a third party external connection, which means that the attacker must take over a third party control system. The third party control system then becomes a more attractive target for the attacker since these systems usually regulate the electrical grid within a given region—raising the potential to affect a wider area.

If the ICS is compromised, most projects will have the ability to manually override the power generation units and maintain control of the spillways, assuming the project has a virtual or physical kill switch that completely disconnects the ICS control capabilities from the units. However, there is a concern that there may be insufficient resources to handle manual operation of remote and multiple sites.

A significant vulnerability at some dam project sites can be attributed to a combination of a lack of cyber and physical security protective measures, as well as an attitude of “security through obscurity” when it comes to ICSs. This concept reflects some operators’ belief that security is present based on the outsider’s lack of knowledge and understanding of a dam project’s complex systems and, therefore, creates a false sense of security based on the premise that the complexity of the system itself is inherently sufficient to deter any type of attack on the system. This is a grave misconception as, normally, this is not the case—especially when the attacker is a nation-state or terrorist organization.

To help reduce the level of vulnerability to a project site, some projects have improved security by disconnecting their ICS from other LANs to create semi-private networks. The use of leased lines or T1 lines for the ICS structure is a good step toward securing systems, especially when used with firewalls and data encryption. However, the lack of security at physical locations that provide access to cyber-related components, (e.g., telephone rooms, cables conduits, switch boards, and LAN connections close to control centers) makes the project vulnerable to intentional insider attack and to accidental contact.

The task of securing legacy assets from cyberattacks will continue to expand and grow even as newer systems are gradually brought online. At some phase in their service life cycle, all ICSs will inevitably assume legacy status. This means that owners and operators will need to plan for maintaining a base level of security through constant technology transition. In short, owners and operators must collectively form an enabling structure that facilitates coordinated security practices and technology uptake processes applicable to both present and future legacy systems. Such an environment is necessary to provide enduring security and keep pace with continuous control system technology and communication improvement cycles.

OTHER SYSTEMS

Levee protection systems can serve as local flood protection (LFP) systems as well as hurricane and storm damage risk reduction systems (HSDRRS). Levee protection systems are typically low in technology integration and most use gravity-gate technology.

The level of sophistication of levee protection systems varies significantly. For instance, many levee protection systems have low-level technology, whereas others encompass SCADA systems that monitor and control multiple pumping stations. Components of levee protection systems that require electrical control systems may include pumping station SCADA, pump, gate, and valve controls, and water level monitoring systems.

Generally, floodgates are left open either for gravity drainage of water or for normal use of navigable waterways. Floodgates are closed either to complete the integrity of the levee system, prepare for an impending flood or hurricane, or to protect areas from more flooding. Pumping stations in the system may include technologically diverse systems for monitoring and controlling capabilities, from low-level technology to SCADA systems.

A variety of Federal, State, local, and private entities gather hydrologic and meteorological data to provide owners and operators and public agencies with some of the tools needed to effectively promote activities that support the environment. The data collected is made available electronically through the use of specialized weather, water, and environmental data collection systems.

For example, the Bureau of Reclamation uses an agricultural weather information system called "AgriMet," with the purpose of promoting water and energy conservation. AgriMet's network consists of more than 90 automated weather stations that collect and telemeter site-specific weather data. AgriMet is strictly a monitoring system consisting of self-contained units that require little maintenance and operate using storage batteries recharged by solar energy.

The data collected from the units is translated into crop-specific water use information. The primary use of the data is for irrigation management (e.g., to supply the amount of water needed by a crop at the optimal time). Other uses of AgriMet data include water management planning for integrated pest management, frost protection, and other crop management activities. Most of this data is provided to users via email and/or to sponsors via view-only workstations.

Similarly, the HydroMet network system is comprised of communications and computer systems that provide information on remotely gathered water and environmental data that is transmitted via radio and satellite to provide near-real-time water management capability. Other information, as available, is integrated with the HydroMet data to provide timely water supply status for river and reservoir operations.

Water quality systems are also used as standalone systems for the management of water and water quality downstream of projects. These systems monitor and maintain water temperature downstream and assist in the gradual release of intake water downstream to help protect fish and other endangered species from dissolved gases and other pollutants in the water. In some large dam projects, water management systems are integrated with ICSs to monitor dissolved gases in water downstream of the hydroelectric power plant and other environmental impacts.

A dam structure monitoring system also represents a stand-alone system designed to aid dam operators at hydropower plants in achieving optimum power generation. This type of system allows the monitoring of stream bank saturation and the control of power generating equipment, allowing a reduction in power generation through the ICS if necessary. The system could feed information into the ICS as a control line to indicate high levels of generation. Even if the system did not have control capabilities, it could function as a "warning system" for the operators.

SECURING INDUSTRIAL CONTROL SYSTEMS IN THE DAMS SECTOR

Identifying the common access points, interconnections, critical cyber elements, and physical components associated with ICSs, as well as understanding the consequences associated with the disruption of each of these elements, is critical to increasing the security posture of the Dams Sector. It is not possible to provide absolute security for all facets of a project. Therefore, it is critical to be able to identify and prioritize the most important assets, and to provide the best level of protection for those assets commensurate with the discernible risk. Therefore, risk analysis is an important criterion in establishing an effective security policy.

IDENTIFICATION OF CRITICAL FUNCTIONS AND OPERATIONS DEPENDENT ON INDUSTRIAL CONTROL SYSTEMS

In order to enhance the Dams Sector's understanding of cyber threats and vulnerabilities, it is critical to identify the hardware, software, networks, communication infrastructure, information, backup systems, and other types of data, which are critical to the operation of an ICS. Identifying critical functions and operations dependent on the ICS should include:

- Location of the cyber assets;
- Cyber asset function;
- System components;
- Devices that aid in securing the asset and/or its perimeter;
- Dependencies;
- Interdependencies;
- Impact in case of loss or failure; and
- Existing protective actions used to secure the asset.

IDENTIFICATION AND SCREENING OF CRITICAL CYBER ELEMENTS

NERC cybersecurity standards define "critical assets" as those "systems and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System" and other critical infrastructure systems. Most standards require documentation of all cyber assets that exist within the electronic security perimeter as a critical cyber asset, and advocate appropriate protection of these assets to ensure the security and integrity. The CIP Standards require that the owner and operator of a facility determine their critical assets and the critical cyber assets associated with them. The definition of critical assets will vary at the project level, district level, and Federal level; therefore, the level of risk associated with the critical asset is determined by the asset owner, to include related public and employee safety.

Normally, dam projects have multiple missions, including flood control, water supply, navigation, and recreation, among others. Dams Sector projects that produce power are also involved in the transport of power and provide operational support for electrical power systems. The Dams Sector recognizes that the CIP Standards apply to all bulk electrical power systems, including hydropower generation facilities.

Each dam project type requires specialized security guidance because of the types of functions they provide. This can be seen when comparing hydropower dams to dams associated with navigation locks: Both projects have unique critical assets and require specialized guidance to protect their respective operations and missions.

It is recognized that cyberattacks could succeed and result in either unauthorized operation of equipment or denial of service. Loss of control and/or monitoring of critical assets would have a significant impact on project reliability, including the ability to restore functions after a partial or total operational shutdown.

Identification of Common Cyber Access Points

To reduce the probability of a successful cyberattack on Dams Sector ICSs, steps must be taken to eliminate potential points of vulnerability. Several of the most common vulnerabilities are discussed below.

- Any unsecured dial-in telephone line is a point of vulnerability. Use of modem dial-back mechanisms and simple ID/password access controls are not sufficient to secure these points of access.
- Malware can be introduced into a system and/or network by someone bringing infected removable media into a facility and inserting it into a PC.
- Malware can also be introduced by electronic mail containing malicious software or a link to the malicious software. Even though this type of infection is well known, it is still one of the most commonly used and successful means of compromising a system.
- A new threat that has emerged recently is the possibility of a Bluetooth-enabled device (cell phone, camera, laptop, or PDA) passing a virus to a device (e.g., a Bluetooth-enabled laptop PC that also has an Ethernet interface) connected to the control system LAN. This problem becomes more apparent as devices are more Bluetooth technology capable, such as printers and scanners. A virus could be passed to these devices and then to a computer on the same network.
- Any Wi-Fi enabled computer with an Ethernet connection enables an attacker to use the Wi-Fi connection to bridge the control system LAN, potentially obtaining the access rights of the owner of the computer via the connectivity.
- An insufficiently protected Wi-Fi AP (access point) and communication ports unnecessarily left open in networks where control systems reside can both be points-of-entry for an attacker. This would give the successful attacker access to the LAN, but additional efforts would be needed to break into the systems.
- Emergency connections, which are normally present in the interconnection of business and control networks, could serve as a potential vulnerability as these connections are normally the paths of least resistance since they are designed to allow quick access to the control network.

The vulnerabilities discussed above are undoubtedly not the only points of vulnerability. However, taking actions to secure these vulnerabilities will greatly reduce the likelihood of a successful attack. There are many well-understood ways in which an attacker could seek to penetrate an ICS. Some of these vulnerabilities assume an inside attacker, others an outside attacker.

There should be no remote access points provided to vendors and/or other support entities to any power generating equipment, spillways, or navigation lock network systems.

Control operators should use a separate Administration LAN or other isolated system for email and other administrative functions. Wherever possible, the ICS should have no connectivity with the Administration LAN or any other network; and alternate methods should be considered to provide operational data to business systems.

INTERCONNECTIONS

All connections between the control system and other LANs/WANs must be adequately protected by firewalls. An insufficiently configured or technically inadequate security control (e.g., a firewall installed without inserting rules for communications; not monitoring the data passing through the firewall) can serve as a point of access for an external attacker.

- The most basic vulnerability of a control system is an insider attack. Such an attack could delete critical primary and backup files or issue commands through an operator console, causing dangerous or destructive control actions.
- If security controls separating the control system network from the corporate network are inadequate, malware can find its way from one system onto the other.
- Just as Wi-Fi access can be used by an attacker to break into the control system network, it can also be used to break into the corporate network.

IDENTIFICATION OF ACCESS POINTS

- Another access point to the ICS is the connection between a control system and another system through a network, such as a backup control system at an alternate control center. Correctly configuring firewalls at every access point and minimizing the number of direct lines between networks is a crucial requirement for the protection of independent networks.
- RTUs are sometimes connected to ICSs by radio or telephone circuits. It has been proven that a person with a radio, a laptop, and commercial software can take control of RTUs and override ICSs. Also, by tapping into a telephone line, the attacker can cut the ICS off entirely and control any RTU on that same telephone line.[h]
- In a geographically distributed corporation, unsecured telephone connections to a corporate network may pose a threat by providing an indirect path for an attacker to reach the control system if the control system is interfaced to the corporate network.
- Corporate Webservers, e-mail servers, and Internet gateways provide access to attackers via the Internet. A simple and effective way to defend against this type of attack is the use of traps to detect, deflect, or counteract attempts at unauthorized entrance into the system.

ASSESSING RISKS OF CRITICAL CYBER ELEMENTS

The NIPP defines risk as a function of consequence, vulnerability, and threat. Many agencies and companies that own or regulate dams in the United States have an extensive background in developing and applying methodologies for assessing risks and prioritizing their asset inventories.

For Dams Sector ICSs, important aspects of risk assessment include determining the value of data flowing from the control network to the corporate network, and determining the security of the remote operation of critical components and of communications systems, etc.

In some situations, risk may be physical or social, rather than purely economic. The risk may be of an unrecoverable consequence, rather than of a temporary financial setback. Effective risk assessments clearly define mitigation cost relative to the effects of the consequence. An accurate risk assessment of critical cyber assets will assist in providing Dams Sector stakeholders with the ability to prioritize

[h] Utility Automation & Engineering T&D, 2007, SCADA Security: 14 Obvious Points of Attack http://www.elp.com/articles/powergrid_international/print/volume-12/issue-6/features/scada-security-14-obvious-points-of-attack.html. (Accessed 1/20/2016).

security needs and focus limited resources on the most urgent security issues. Risk assessment data is also necessary in building a sound business case for investment in creating, procuring, and implementing control system security measures.

Dams Sector owners and operators can utilize this approach to identify assets, systems, and networks; and to collect information pertinent to risk management. Their focus should be on those assets, systems, and networks which, if affected, would result in significant consequences— such as impacts on national economic security, national public health and safety, public confidence, and loss of life. The results of this approach should drive the Dams Sector's risk-reduction and management activities.[i]

To prioritize critical ICS equipment within the Dams Sector, it is essential to first identify and define the Sector's most critical cyber assets.

THREAT CONSIDERATIONS

The pervasive use of technology, combined with the drive for ubiquitous connectivity and reduction in human oversight in ICSs, has created significant vulnerabilities in all types of critical infrastructures. Cyberattack tools are increasing in sophistication and ease of use, threatening to outpace security efforts for ICSs.

The U.S. Department of Energy's National SCADA Test Bed program funded 12 separate control system security reviews. During these reviews, experts from the Idaho National Laboratory found that all of the evaluated systems suffered from high-impact security vulnerabilities that could be exploited by a low-skill attacker using techniques that do not require physical access to systems. In reviewing the design and implementation of these control systems, the team discovered that enhanced security controls cannot easily be implemented in currently deployed systems while still assuring basic system functionality.

All configuration management (e.g., version control, patches, system upgrades, data and hardware backup, etc.) should be supported by the designated authority at the corporate office. The requirements of the plan should encompass, but not be limited to, IP traffic, illegal broadcasting, and activity or audit logs. Any of these configurations should be fully tested on a test system that replicates the project's ICS before it is deployed in the live production system. In addition, no network links to the ICS from the corporate office should be in place.

In many cases, a project includes one main control center with no main backup control center. However, there may be several support workstations within the project that could be utilized as a backup control center. The primary intent of the support workstation is to be used in a view-only mode for monitoring and diagnostics; however, it could be utilized as a backup control center if necessary.

Computer attackers are constantly looking for new targets and follow the path of least resistance, which could lead them to the ICSs that underlie our critical infrastructures. Information security experts agree that, without implementing risk mitigations, ICSs will continue to be vulnerable.

Based on historical and current cybersecurity incident trends in other technology domains, the corrections will most likely begin with small-scale incidents focused on economic gain, followed by

[i] DHS, 2013, National Infrastructure Protection Plan: 2013 [http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf] (Accessed 1/20/2016)

the release of publicly available vulnerability discovery tools, and then a transition to large-scale incidents designed to reduce confidence in the infrastructure systems.[j]

The general threat environment for the Dams Sector is highly variable. Historically, threats to dams in the United States have been limited to demonstrations, vandalism, and minor criminal activities. With the advent of the Internet and open digital communication, the threat to dams today can come from cyberattacks on ICSs that monitor and control essential elements of dam operations. Developing a clear understanding of threats is a fundamental element of vulnerability assessment and risk management. Threats, threat trends, tactics, and motivations should be characterized. To the extent possible, characterization of the threat environment should be localized to the facility area.

Cyber threats to ICSs refer to persons who attempt unauthorized access to ICS devices and/or networks using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet or other communication path. Threats to Dams Sector ICSs can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders, including:

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- Insiders
- Phishers
- Spammers
- Spyware/Malware Authors[k]

These threat vectors, combined with insider threat and a range of other pervasive cyber threats to critical infrastructure, highlight the need for public, private, academic, and international entities to collaborate and enhance cybersecurity awareness and preparedness efforts, and to ensure that the cyber elements of critical infrastructure are:

- Robust enough to withstand attacks without incurring catastrophic damage;
- Resilient enough to sustain nationally critical operations; and
- Responsive enough to recover from attacks in a timely manner.

[j] Idaho National Laboratory, Mr. Aaron R. Turner - 2007, House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science & Technology - Hearing on “Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure,” https://chsdemocrats.house.gov/SiteDocuments/20070419153130-95132.pdf (Accessed 1/20/2016)

[k] US-CERT, 2009, Cyberthreat Source Descriptions, http://www.us-cert.gov/control_systems/csthreats.html (Accessed 1/20/2016)

CONSEQUENCE ASSESSMENT

Dams Sector stakeholders must consider potential consequences associated with ICS intrusion. Adversaries identify and exploit vulnerabilities to execute attacks, and the effects of those attacks become one or more consequences. Well-defined policies and procedures lead to mitigation techniques designed to thwart attacks—managing risk to eliminate or minimize consequences. The degradation of dam operations, economic status, or national confidence could all justify mitigation. The fiscal justification for mitigation must be determined from a benefit-cost ratio analysis which includes the effects of the following:

- **Public Health and Safety** - Effect on human life and physical well-being (e.g., fatalities, injuries/illness);
- **Economic -** Direct and indirect economic losses (e.g., cost to rebuild asset, cost to respond to and recover from attack or incident, downstream costs resulting from disruption of product or service, or long-term costs due to environmental damage);
- **Psychological -** Effect on public morale and confidence in national economic and political institutions (encompassing changes in perception that emerge after a significant incident that affects the public's sense of safety and well-being, and which may be manifest in aberrant behavior); and
- **Government/Mission Impact -** Effect on government's or industry's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

An assessment of consequences in all these categories may be beyond the capabilities and resources typically available to Sector owners and operators. At a minimum, consequence assessments should focus on the two most fundamental impacts: public health and safety and the most relevant direct economic impacts.

VULNERABILITY ANALYSIS

ICS are vulnerable to cyberattack from inside and outside the control system network. To understand the vulnerabilities associated with ICSs, Sector owners and operators should review the types of communications and operations associated with the control system, as well as have an understanding of how attackers are using system vulnerabilities to their advantage. It is recommended that understanding control system cyber vulnerabilities should include the following analyses:

- Access to Control System LAN
- Common Network Architectures
- Dial-up Access to RTUs
- Vendor Support
- IT Controlled Communication Gear
- Corporate VPNs
- Database Links
- Poorly Configured Firewalls
- Peer Utility Links
- Discovery of the Process

- Control of the Process
- Sending Commands Directly to Data Acquisition Equipment
- Exporting the HMI Screen
- Changing the Database
- Man-in-the-Middle Attacks[1]
- Distributed Denial of Service (DDoS)

APPROACHES FOR PRIORITIZING CRITICAL CYBER ELEMENTS

The NIPP provides a methodical approach to a risk analysis and management framework (Figure 4) that establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector risk. These processes can readily be applied as an approach to prioritization of critical cyber and ICS elements of the Dams Sector.

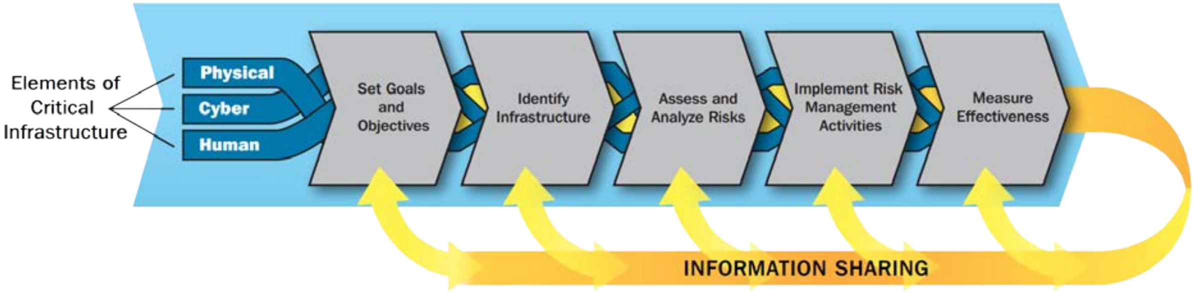


Figure 4: NIPP Risk Management Framework (Source: NIPP 2013)

The risk management framework is organized to promote overall sector protection by

- Focusing activities on efforts to set goals and objectives;
- Identifying assets, systems, and networks;
- Assessing risk based on consequences, vulnerabilities, and threats;
- Establishing priorities based on risk assessments; and
- Implementing protective programs and resilience strategies that measure effectiveness and return-on-investment related to risk.

[1] US-CERT, 2009, Overview of Cyber Vulnerabilities, http://www.us-cert.gov/control_systems/csvuls.html (Accessed 1/20/2016).

SUMMARY OF SECTOR CHALLENGES AND DEVELOPMENT

COST/BENEFIT ANALYSIS

Developing and integrating security advances into ICS architectures can be extremely expensive. These costs can be difficult to justify, particularly because threats are not easily identified or modeled, and the Dams Sector has yet to experience a major cyberattack. Without sufficient means to fully quantify and demonstrate the potential impacts of cyberattacks on Dams Sector ICSs, owners and operators are hard-pressed to justify ICS security as a top funding priority. Industry stakeholders must cooperate to organize a strategic paradigm shift among key decision-makers, ultimately leading to a more proactive approach supporting ICS cybersecurity advances.

CONSEQUENCE MITIGATION APPROACHES

By systematically documenting and prioritizing known and suspected control system vulnerabilities and their potential consequences, Dams Sector owners and operators will be better prepared to anticipate and respond to present and future threats. Risk identification will provide the necessary foundation for a solid cybersecurity strategy and enable the Dams Sector to more effectively implement mitigation and response plans to improve system reliability and resilience over the long term.

Much of the ICS security effort is based upon three guiding principles: *Protect*, *Detect*, and *Respond*.

- ***Protect* -** To deploy specific protection measures to prevent and discourage electronic attack against the ICS.
- ***Detect* -** To establish mechanisms for rapidly identifying actual or suspected electronic attacks.
- ***Respond* -** To undertake appropriate action in response to confirmed security incidents against the ICS process.

Where a single protection measure has been deployed to protect a system, there is a risk that, if a weakness in that measure is identified and exploited, there will effectively be no protection provided. No single security measure can be considered foolproof as vulnerabilities and weaknesses are continuously being discovered. In order to reduce these risks and to avoid single points of failure, multiple protection measures should be implemented in series.

In order to safeguard process control systems from electronic attacks see NIST 800-82 or visit: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf for a description of *Defense in Depth Strategies*.

When implementing security measures, there is a tendency to focus the majority of efforts on the technology elements. Although important, technology is insufficient on its own to provide robust protection. For example, when implementing a firewall, it is not just a matter of installation and configuration; consideration must also be given to associated procedural and managerial requirements.

- Procedural requirements may include changing control and firewall monitoring.
- Managerial requirements may include firewall assurance, standards, and training.

RESEARCH & DEVELOPMENT NEEDS AND CONSIDERATIONS

In order to enhance and sustain ICS security and resilience, one of the Dams Sector goals is to identify R&D security technology needs, priorities, and achievements. R&D serves to improve cybersecurity protective capabilities and dramatically lowers the cost of existing capabilities so that State, local, tribal, territorial, and private sector partners can afford to do more within limited budgets.

To achieve this goal, it is critical to leverage resources and capabilities among utilities, associations, vendors, communities, government organizations, and others in improving the Dams Sector's ability to prepare and respond to cyber events. Engaging these groups through outreach mechanisms will encourage them to quickly implement new risk mitigation measures and provide input from the field to help guide future technology development.

For example, such programs can provide:

- Measurable demand for new, more secure products from vendors;
- Support for sector-specific patch testing protocols;
- Development of intrusion detection and intrusion protection systems, leveraging efforts currently underway in the I3P program;
- Opportunities to work with vendors to improve the authentication protocols in their products;
- Encouragement for vendors to design products with limited service capability to reduce vulnerabilities and enhance security of available ports;
- Unified support for approaching NERC for changes in CIP requirements; and
- Input for use by vendors currently developing components for use in a wireless environment.

A steady communication with Federal entities and the general public will sustain support for future investments in cybersecurity. The future of ICS security depends on public and private Dams Sector stakeholders coming together to work toward common goals. This ongoing collaboration will accelerate and sustain ICS security advances in the Dams Sector and the critical infrastructures that rely on the assets within the Dams Sector.

KEY CHALLENGES

Challenges to cybersecurity consist of not only the direct risk factors that increase the probability of a successful attack and the severity of the consequences, but also of those factors that limit the ability to implement ideal security enhancements.

Challenges related to the implementation of security measures include organizational, institutional, economic, and technical factors that either limit the availability of security measures or increase the difficulty of implementing optimum security enhancements. Several examples of these challenges:

- Business cases for control system security have not been developed,
- Clear and specific up front security requirements are lacking,
- There is limited understanding of cybersecurity risks,
- There has been a rapid change in threat actors and vulnerabilities,
- There are limited resources to mitigate risks,
- Integration of new technologies into legacy systems is difficult or impossible in some cases,
- It is difficult to manage changes in an organization's mission,

- There are differing viewpoints of priorities within the Sector, and
- It is difficult to fully implement cybersecurity across the Dams Sector.

In addition, there are a number of industry trends within the Sector that present challenges to ICS security, including the increasing implementation of automation over manually-controlled systems, as well as replacing manual systems with intelligent electronic devices. Although these trends are cost-effective and improve efficiency by limiting human error, they also limit opportunities to mitigate the effects of an incident through human oversight.

Awareness and understanding of the need for cybersecurity also presents a challenge to both government and industry. Although cybersecurity requires significant investments in time and resources, an effective cybersecurity program may reduce the likelihood of a successful cyberattack or reduce its impact. Network disruptions resulting from cyberattacks can lead to loss of money, time, products, reputation, sensitive information, or even life through cascading effects on critical systems and infrastructure. From an economic perspective, cyberattacks have resulted in business losses and damages valued in billions of dollars.

A significant piece of this challenge is the need for owners and operators to make risk management decisions, including those for cybersecurity, based on a return on investment and the desire to ensure business continuity. Market-based incentives for cybersecurity investments include protection of intellectual capital, security-influenced procurement, market differentiation, and public confidence. Sometimes, however, cyber assets, systems, or networks may be deemed to be nationally critical and necessitate additional risk management beyond that which the private sector implements as part of their corporate responsibility.

Path Forward Solutions and Next Steps

The intent of this Roadmap is to encourage Dams Sector stakeholders to develop a set of milestones, to create challenges to achieve the milestones, and to devise potential solutions to overcoming the barriers to cybersecurity. This Roadmap should be further developed to help identify Sector challenges and opportunities to secure ICSs. The developed Roadmap needs to be publicized and easily accessible to enhance information sharing and partnership.

While the precise roles and responsibilities of organizations in implementing this Roadmap have not yet been fully defined, these roles should mature and evolve as the Roadmap is disseminated and reviewed by those engaged. The Roadmap socialization process should include motivating industry leaders to step forward and initiate the most time-sensitive activities.

The contributors to this Roadmap encourage organizations and individuals to participate in ways that will best capitalize on their distinct skills, capabilities, and resources for developing the potential solutions described herein. This affords companies and organizations the flexibility to pursue projects that correspond to their unique interests. In addition, continuous improvements will be driven by information sharing and coordination supporting the identification and development of efficient solutions in an environment consisting of multiple governing and regulatory agencies, independent facilities, and a variety of vendors and R&D organizations. However, without a unified structure, it will be difficult to adequately identify, organize, fund, and track the diverse activities and their corresponding benefits.

Dams Sector stakeholders must clearly define the desired outcomes, resources, and capabilities required, as well as determine how the results will contribute to addressing particular challenges in the Roadmap, identifying gaps, and coordinating the development and initiation of new Roadmap activities.

To sustain the efforts of this Roadmap, the risk management planning process must include constant exploration of emerging ICS security capabilities, vulnerabilities, consequences, and threats. The ICS security objectives outlined in this Roadmap are intentionally broad-based and, therefore, the specific details of assessing risk and employing appropriate risk mitigation strategies may later be developed in an appropriate technical plan. As the Dams Sector pursues the strategies contained in the Roadmap and potential technical plan, it will continue to review, assess, and adjust the mix of activities that will improve ICS security today and in the future.