Dams Sector

Roadmap to Secure Control Systems

2010

Homeland Security

Foreword

The Dams Sector Roadmap to Secure Control Systems describes a plan for voluntarily improving 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 communicate recommended strategies for improvement within their 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 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 U.S. Department of Homeland Security's Office of Infrastructure Protection and the National Cyber Security Division 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-Specific Agency Executive Management Office, Dams Sector Branch, would like to acknowledge the Dams Sector Council members for their contributions in the development of the Dams Sector Roadmap to Secure Control Systems.

Executive Summary

The Dams Sector Roadmap to Secure Control Systems describes a plan and strategic vision for voluntarily improving the cybersecurity posture of control systems within the Dams Sector. Designing, operating, and maintaining a facility to meet essential reliability, safety, and security needs require 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. 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 the cyber issues of control systems.

Many of the control systems used today were initially designed for operability and reliability during an era when security received low priority. 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. However, newer control systems are highly network-based and use common and open standards for communication protocols; this interoperability 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 cyber attack and the factors that limit the ability to implement ideal security enhancements. A majority of 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 cyber attack. 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 will 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 the 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 the information will be used, disseminated, and protected. Possibly, as a result of this lack of information sharing, the return on investment for vendors to sustain control system and security tool improvement, including R&D to advance the technology, is unclear. A further complication is that vendors currently do not have adequate requirements or standards to design, build and maintain cybersecurity into 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 lifecycles.

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. These challenges include developing mitigating solutions, defining longer-term needs, and articulating control system security guidelines and practices for improvement.

Table of Contents

1. Introduction

Leaders from the nation's CIKR 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 cyber attacks 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 an opportunity for industry and government experts within a sector to collectively address issues concerning the state of control system cybersecurity and appropriate strategies for securing their sector. 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 include control system vendors, system integrators, and academia, which 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 organizations 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.

The 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; 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 and 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 Chapter 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.

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 a vision, along with a supporting framework 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 over the next 10 years;

Roadmap Purpose

- Present the Dams Sector's security vision
- Define a consensus-based stategy 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

- Proposes methods and programs that encourage participation of all stakeholders;
- Guides efforts by industry, academia, and government;
- Identifies opportunities for cooperative work across sectors in cybersecurity awareness, training and information sharing;
- Promotes continuous improvement in the security posture of control systems within the sector;
- Strengthens government programs designed to improve the protection of control systems; and
- Supports the implementation of the goals included 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 CIKR. 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 to meet 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, however those impacts can 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 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 Internet to the extent they are connected to control systems. Securing access to and control of the business network and Internet is generally the responsibility of information technology (IT) personnel, and thus 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 Internet connections 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 resulting from cyber compromise is one of the principal factors contributing to control systems risk. This roadmap includes both of these factors in understanding and planning for cybersecurity enhancements; however, actual engagement in describing physical access control and physical consequence management is outside the scope of this roadmap.

This roadmap covers 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

Homeland Security Presidential Directive 7 (HSPD-7) Critical Infrastructure Identification, Prioritization, and Protection, required the development of the NIPP to provide the collaborative framework and unifying structure for the integration of existing and future CIKR protection efforts for the government and private sector.

HSPD-7 also assigned Sector-Specific Agencies (SSAs) for each of the CIKR sectors, as the lead agencies responsible for collaborating with other Federal, State, local, tribal, territorial, and private sector partners. SSAs among other things, implement and encourage the development of information sharing and analysis mechanisms, including the sharing of information regarding physical and cyber threats, vulnerabilities, incidents, potential protective measures, and accepted industry practices. The Office of Infrastructure Protection (IP) within DHS serves as the SSA for the Dams Sector.

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 CIKR protection. The CIPAC consists of Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC).

SCCs are self-organized, self-run, and self-governed 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 CIKR sectors as well as with DHS, Federal Energy Regulatory Commission (FERC), and other government agencies, including the Dams GCC.

The Dams Sector GCC acts as the government counterpart and partner to the SCC to plan, implement, and execute sector-wide security programs for the sector's assets. It comprises representatives from across 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, in 2004 the DHS National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP), 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 HSPD-7, the Dams Sector is also required to develop and maintain a SSP that details the sector's plans to protect human resources, cyber systems, and physical assets. The Dams Sector Roadmap to Secure Control Systems provides a logical and cohesive framework to design and implement a strategy to carry 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 action 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 accomplished over the next 10 years to achieve the outlined goals and vision. While it contains many actionable items, as a plan, it is only useful to the extent that financial resources and leadership 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, mine tailings and other industrial waste impoundments, or other similar water retention and 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 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 flow. This information is then converted to electrical signals for processing and, if needed, enables corrective actions to be taken automatically or with human interaction.

Within the Dams Sector, the term "control system" is frequently interchanged 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, it 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 comprise non-electronic relay-based components without cyber assets connected to them, therefore having a low risk of being affected in the occurrence of a cyber event.

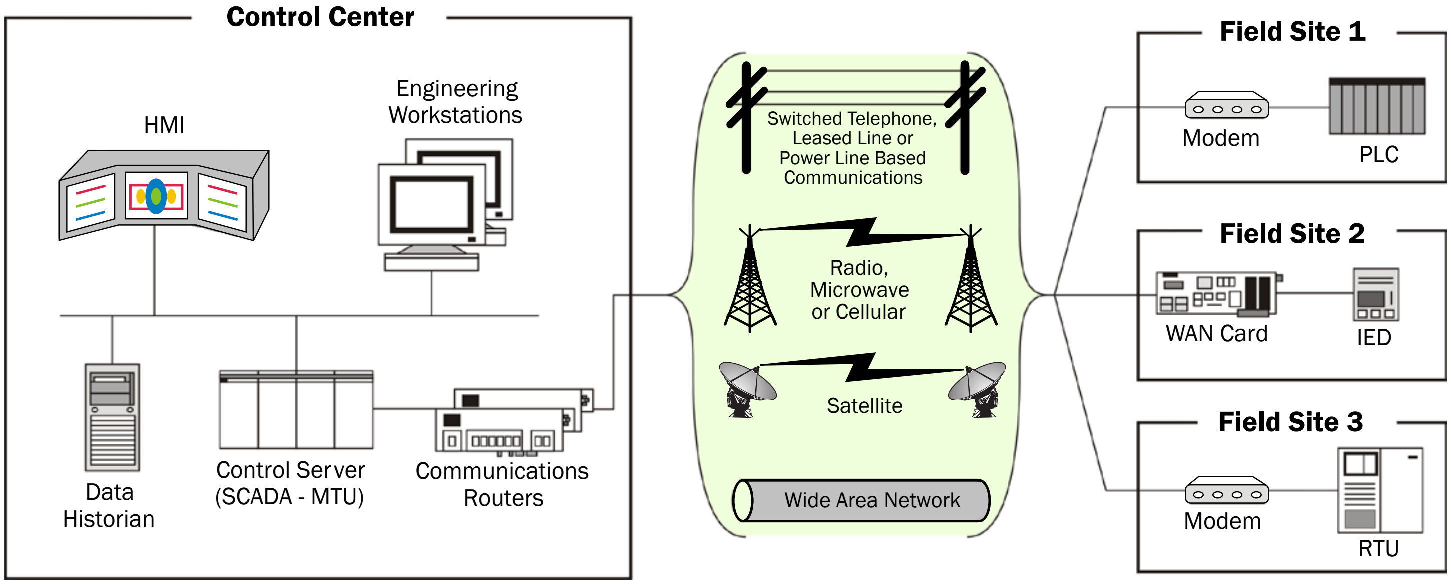
Many of the ICS used today were designed for operability and reliability during an era when security received low priority. These systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and/or communications technologies. Infiltrating and compromising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

In contrast, newer ICS are highly network-based and use common and open standards for 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, which 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, or cable or wireless networks are often used. A typical system configuration is shown in Figure 1.

The potential for system accessibility resulting from this interoperability exposes network assets to cyber infiltration and subsequent manipulation of sensitive operations. Furthermore, increasingly sophisticated cyber attack 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 ICS are quite reliable, security policies and practices are often undependable. Detailed analyses of the 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 ICS from cyber risks has become more difficult. Some of the most serious security issues inherent in current ICS, related to the increased ICS vulnerability to threats, include:

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



- **Increased Connectivity.** Today's ICS are being increasingly connected to company business systems that rely on common operating platforms and are accessible through the Internet. Even though these changes improve operability, they also create serious vulnerabilities because improvements in the security features of ICS outpace those platforms.
- **Interdependencies.** Due to the high degree of interdependency among infrastructure sectors, failures within one sector can spread into others. A successful cyber attack may be able to take advantage of these interdependencies to produce cascading impacts and amplify the overall economic damage.
- **Complexity.** The demand for real-time control has increased system complexity in several ways. Access to ICS is being granted to more users; business and ICS 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.
- **Wireless Connection & Communication.** Even limited connection to the Internet exposes ICS 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.

Protection Issues

- Increased connectivity
- Interdependencies
- Complexity
- Legacy systems
- Wireless Connection & Communication
- Offshore reliance
- Information availability

- **Offshore Reliance.** There are no feasible alternatives to the use of COTS products in ICS. 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 ICS; 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.

A more in-depth description of typical ICS 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 ICS (ICS) Security, Recommendations of the National Institute of Standards and Technology."

Key Stakeholders

ICS security is a shared responsibility among 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 CIKR. Key stakeholder groups and sample members include:

- *Asset owners and operators* ensure that ICS are secure by making the 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*, funded by government and industry that explore long-term security solutions, develop new tools, and address solutions for ICS system vulnerabilities, hardware, and software; and
- *Universities and colleges*, chartered to provide education for future generations, ideally provide courses and degrees that satisfy the needs and requests of industry.

A Framework For Securing Control Systems

Protecting infrastructure ICS 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 a framework 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 the challenges and assist in meeting the goals.

Vision

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

> ***Within 10 years, control systems throughout the Dams Sector will be able to operate securely, robustly, resiliently, and be 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 framework 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 manner and to mitigate cybersecurity problems in a rational manner.

Control Systems Security Goals

Today's ICS 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, applying security tools and practices, and considering security as they procure and install next-generation systems.

Attention to ICS cybersecurity has been increasing over the past several years. 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 rather classical security models that measure and assess, protect, detect, defend (detain or eliminate as may be required), recover, build-in security (rather than attaching it as an after-thought), and 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 in the future to ensure continuing fixes as needs arise. 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 produced systems. The following list briefly describes each goal:

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. Within 10 years, the sector will help ensure that owners and operators have the ability and commitment to perform fully automated security state monitoring of their control system networks, with real-time remediation.

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 as follows:

1) Isolating the control system from all other business or commercial communications channels;
2) Utilizing serial channels;
3) Employing passive file transfer solutions; and
4) Using appropriate communications protocols/firewalls/demilitarized zones for external connectivity.

Appropriate security solutions will 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, they will be replaced or upgraded with next-generation control system components and architectures that offer built-in, end-to-end security. This replacement will typically not be driven solely by security-related concerns.

Detect intrusion and implement response strategies. Cyber intrusion tools are becoming sophisticated to the degree that any system can become vulnerable to emerging threats. Within 10 years, the Dams Sector will be operating networks that automatically provide contingency and remedial actions in response to attempted intrusions.

Sustain security improvements. Maintaining aggressive and proactive cybersecurity of ICS 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 a sustained advancement in securing their ICS.

Secure by design. ICS products will be secure-by-design within 10 years. Dams Sector owners and operators will insist, through specifications and orders, that vendors provide systems that are secure-by-design and will work with vendors to achieve this goal.

These goals provide a logical framework 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.

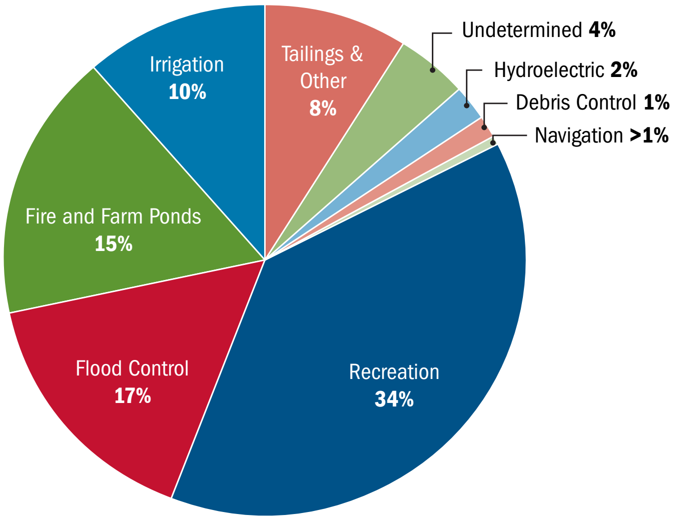
Background

As previously referenced, the NIPP provides the unifying structure for the integration of CIKR protection and resilience efforts as part of a coordinated national program. The NIPP includes 18 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. Figure 2 shows the distribution of dams by function.

Figure 2: Distribution of Dams by Primary Purpose



Some 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 American cropland is irrigated by using water stored behind dams and thousands of jobs are tied to producing crops grown with irrigation water;
- **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 produce more than 270,000 gigawatt hours, contributing 7 percent of the Nation's electricity and representing 70 percent of the Nation's renewable energy generation;
- **"Black Start" Capabilities:** There are 4,316 megawatts of "incremental" hydropower available at sites with existing hydroelectric facilities. Incremental hydropower is defined as capacity additions or improved efficiency at existing hydro projects. 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 Americans;
- **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 provided at hydropower projects licensed by the Federal Energy Regulatory Commission (FERC). In addition, about 400 million people annually visit a project of the U.S. Army Corps of Engineers (USACE), and about 90 million visit a project 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 intracoastal navigation system is the ability to efficiently convey large volumes of bulk commodities moving long distances. If the cargo transported on the inland waterways each year had to be moved by another mode, it would take an additional 6.3 million rail cars or 25.2 million trucks to carry the load. The ability to move more cargo per shipment makes barge transport 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; and
- **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.

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

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 from 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, failures within one sector can spread into others. A successful cyber attack may be able to take advantage of these relationships to produce cascading impacts and amplify the 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;
- The Water Sector supplies potable water stored by dams to concentrated populations and commercial facilities in the U.S.;
- The Energy Sector provides approximately 8 to 12 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 destruction, including loss of life, massive property damage, and severe long-term consequences. A successful cyber attack could affect dam operations in a variety of ways, some with potentially devastating repercussions. An attack could:

- Disrupt the operation of ICS by delaying, blocking, or shutting down the flow of information, thereby denying network availability to dam control system operators;
- Send false information to control system operators, either to disguise unauthorized changes or to initiate inappropriate actions by automated ICS operators;
- 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, resulting in the potential damage to equipment;
- Make unauthorized changes to programmed instructions in controllers, change alarm thresholds, order premature shutdown of processes (such as prematurely shutting down generators, operating or disabling sluice and spill gates, control valves, etc.) or even disable control and safety equipment;
- Interfere with the operation or security systems of nearby projects by using the attacked project's system as a cover; and
- Disrupt the quality of electrical services.

Sector Regulations

In the United States, the safety of dams is regulated by a number of different agencies. Many facilities throughout the Dams Sector are multi-purpose, and therefore must adhere to multiple standards corresponding to the different operations the facility provides. The agency or agencies that maintain regulatory oversight of a dam can also depend on the ownership as well as its purpose. For example, the U.S. Bureau of Reclamation (Reclamation) and USACE each self-regulates its projects.

Within the Dams Sector, non-Federal dams that produce hydroelectric power are regulated by FERC and/or State dam safety offices. Federally owned dams are self-regulated, and most non-Federal/non-hydropower dams are regulated by State dam safety offices.

[a] Department of Homeland Security, 2008, National Infrastructure Protection Plan - Dams Sector, **http://www.dhs.gov/xlibrary/assets/nipp_snapshot_dams.pdf.**

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. NERC has been a driver in establishing cybersecurity standards that are used to meet FERC requirements.

In response to the power blackout in 2003 in the northeastern United States, NERC promoted the development of a new mandatory system of reliability standards and compliance that would be backstopped by FERC. These standards would focus on ensuring all entities responsible for the reliability of the bulk electric systems in the United States identify and protect critical cyber assets that control or could impact the reliability of those systems.

In August 2003, an interim "urgent action" cybersecurity standard (designated UA 1200) was initially adopted by NERC, and later proposed as a permanent standard (designated NERC 1300) in August 2005. In May 2006, a revised and modified version of NERC1300 was developed under NERC's American National Standards Institute accredited process (which incorporated thousands of comments from experts and operations personnel) and was subsequently adopted by NERC as the Critical Infrastructure Protection (CIP) Reliability Standards, CIP-001 through CIP-009.

In January 2008, FERC issued Order 706, "Mandatory Reliability Standards for Critical Infrastructure," which approved eight CIP Reliability Standards, CIP-002 through CIP-009[b] (CIP-001 was previously approved). The CIP standards are mandatory and require bulk power system users, owners, and operators, including hydroelectric power plants in the U.S., 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.

Descriptions of the CIP standards are provided below. As these standards may be subject to future revision, the suffix that denotes the revision status (e.g., -2) is not included in the list:

- CIP-001 - **Sabotage Reporting:** Requires a responsible entity to define, process and track disturbances or unusual occurrences, suspected or determined to be caused by sabotage and shall report to appropriate governmental agencies and/or regulatory bodies.
- CIP-002 - **Critical Cyber Asset Identification:** Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.
- CIP-003 - **Security Management Controls:** Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002.
- CIP-004 - **Personnel and Training:** Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.
- CIP-005 - **Electronic Security Perimeters:** Requires the identification and protection of an electronic security perimeter and access points. The electronic perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002.
- CIP-006 - **Physical Security of Critical Cyber Assets:** Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic perimeter are kept in an identified physical security perimeter.
- CIP-007 - **Systems Security Management:** Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.
- CIP-008 - **Incident Reporting and Response Planning:** Requires a responsible entity to identify, classify, respond to, and report cybersecurity incidents related to critical cyber assets.
- CIP-009 - **Recovery Plans for Critical Cyber Assets:** Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recover techniques and practices.

Other cybersecurity guidelines developed, such as those by NIST (National Institute of Standards and Technology) specified under the NIST Special Publication (SP) 800-53 "Recommended Security Controls for Federal Information Systems" and NIST SP 800-82 standards "Guide to Industrial Control Systems Security" generally offer more granularities in the context of defining an electronic security perimeter around ICS assets. NIST SP 800-53 was originally developed to apply to traditional government-operated IT systems and contains specifications for information security controls that are binding for all non-national security information and information systems belonging to, or operated for, Federal agencies. However, NIST SP 800-53 has also been used in non-government IT and control system environments.

[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/page.php?cid=2|20.**

As part of the ongoing initiative to develop a unified information security framework for the Federal government and its contractors, NIST SP 800-53 revision 3 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 standardized set of management, operational, and technical controls provides a common specification language for securing Federal information systems processing, storing, and transmitting national security and non-national security information. The revised security control catalog also includes state-of-practice safeguards and countermeasures needed by organizations to address advanced cyber threats capable of exploiting vulnerabilities in Federal information and ICS. In 2006, NIST also established the "Industrial Control System Security Project" to improve the security of public and private sector ICS; a major part of the project is to research the applicability of SP 800-53 to ICS and to clarify/rectify any problems experienced in applying SP 800-53 to ICS.

NIST standards are mandatory for Federal facilities under the Federal Information Security Management Act (FISMA) guidelines. The Federal Information Security Management Act of 2002 ("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.

Since the NIST cybersecurity guidelines specified under the NIST SP 800-53 revision 3 and NIST SP 800-82 standards offer more granularities in the context of defining an electronic security perimeter around ICS assets, Dams Sector owners and operators believe that the NIST guidelines, rather than the CIP Standards, lead to better results with respect to hardening control systems. In addition, the NIST standards allow owners and operators to use a risk-based approach when meeting the standards, whereas the mandatory CIP Standards are primarily focused on compliance with pre-established requirements, which may not be compatible with a risk-informed, site-specific analysis.

The CIP Standards, to which the hydropower facilities within the Dams Sector must comply, present a number of significant challenges to sector stakeholders. Interpretation of the requirements and application to the specific realities of Dams Sector facilities is difficult as many facilities are confronted with compliance requirements for multiple standards, some of which are conflicting. Owners and operators believe that the lack of clear and established policies and guidelines associated with the CIP Standards makes their implementation difficult because of conflicting interpretations. These concerns were apparent during the "Dams Sector Cybersecurity Summit" conducted on June 24-25, 2009 in Chicago, IL, which was organized to provide industry and government experts with the opportunity to discuss the most significant issues and concerns regarding cybersecurity and control systems.

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 physical and cybersecurity) 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 cyber attack. This represents an overarching concern of the sector since costly fines are levied for non-compliance with the standards.

During the cybersecurity summit, participants also strongly highlighted the need to develop guidance in order to ensure owners and operators understand the CIP Standards and its applicability to their respective facilities, as well as recommendations pertaining to the implementation process to ensure compliance is achieved. Furthermore, there is a need to develop guidance for owners and operators that addresses the potential implications of future requirements as they are identified.

Dams Sector Cybersecurity Coordination

As previously referenced, the NIPP relies heavily on the sector partnership framework as the primary organizational structure for coordinating CIKR 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 protection and resilience of physical, human, and cyber infrastructure 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 SCC currently consists of the following industries, trade associations, and other dam stakeholders:

- Allegheny Energy
- Ameren Services Company
- American Electric Power
- Association of State Dam Safety Officials
- Association of State Floodplain Managers
- AVISTA Utilities
- CMS Energy
- Colorado River Energy Distributors Association
- Dominion Resources
- Duke Energy
- Exelon Corporation
- Hydro-Quebec
- National Association of Flood and Stormwater Management Agencies
- National Hydropower Association
- National Mining Association (ex-officio member)
- National Water Resources Association
- New York City Department of Environmental Protection (ex-officio member)
- New York Power Authority
- Ontario Power Generation
- Pacific Gas and Electric Company
- PPL Corporation
- Progress Energy
- Public Utility District 1 of Chelan County, Washington
- Scana Corporation
- Seattle City Light
- South Carolina Public Service Authority (Santee-Cooper)
- Southern California Edison (ex-officio member)
- Southern Company Generation
- United States Society on Dams
- Xcel Energy

Dams Government Coordinating Council

The Dams GCC currently consists of the following Federal, State, local, tribal, and territorial government entities:

- Bonneville Power Administration
- Environmental Protection Agency
- Federal Energy Regulatory Commission
- Tennessee Valley Authority
- State of California, Department of Water Resources
- State of Colorado, Division of Water Resources
- State of Nebraska, Department of Natural Resources
- State of New Jersey, Department of Environmental Protection
- State of North Carolina, Department of Environment and Natural Resources
- State of Ohio, Department of Natural Resources
- State of Pennsylvania, Department of Environmental Protection
- State of Washington, Department of Ecology
- US Department of Agriculture, Natural Resources Conservation Service
- US Department of Commerce, National Weather Service
- US Department of Energy
- US Department of Defense, U.S. Army Corps of Engineers
- US Department of Homeland Security, Office of Infrastructure Protection
- US Department of Homeland Security, Federal Emergency Management Agency
- US Department of Homeland Security, US Coast Guard
- US Department of Homeland Security, Science and Technology Directorate
- US Department of the Interior, Bureau of Reclamation
- US Department of Labor, Mine Safety and Health Administration
- US Department of State, International Boundary and Water Commission
- Western Area Power Administration

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:

- American Society of Civil Engineers (ex officio)
- Association of State Floodplain Managers
- State of California, Department of Water Resources
- FM Global (ex officio)
- Los Angeles County Department of Public Works

- Louisiana State Police, Levee District
- Metropolitan Water District of Southern California
- National Association of Flood and Stormwater Management Agencies
- Reclamation District 1000, Sacramento, CA
- Southeast Louisiana Flood Protection Authority
- South Florida Water Management District
- South La Foursche Levee District, Galiano, LA
- U.S. Society on Dams

Levee Sub-Sector Government Coordinating Council

In addition, a Levee Sub-Sector Government Coordinating Council (LGCC) was 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 government agencies.

The LGCC currently consists of the following members:

- State of California, Department of Water Resources
- US Department of Defense, U.S. Army Corps of Engineers
- US Department of Agriculture, Natural Resources Conservation Service
- US Department of Homeland Security, Office of Infrastructure Protection
- US Department of Homeland Security, Federal Emergency Management Agency
- US Department of State, International Boundary and Water Commission

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 issues. In addition, the US-CERT and the Industrial Control System Cyber Emergency Response Team (ICS-CERT), which are also DHS organizations, provide cybersecurity information along with the State organization—Multi-State Information Sharing and Analysis Center (MS-ISAC), described below.

Cross-Sector Cybersecurity Working Group

As with the SCCs and GCCs, the 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 CIKR 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 CIKR, 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 ICSJWG also operates under the auspices of CIPAC and was established in December 2008. The ICSJWG is a collaborative coordination body operating under CIPAC. It was established to facilitate the collaboration of ICS stakeholders and to accelerate the design, development, and deployment of enhanced security for ICS. ICSJWG participants include international stakeholders, government, academia, owner/operators, systems integrators, and the ICS vendor community. Although its objective is to reduce the risk of cyber ICS, which is the same as that of this roadmap, the ICSJWG scope is coordination across all CIKR Sectors, whereas this roadmap's focus is within the Dams Sector. Members of the Dams Sector Councils also are active members of the ICSJWG.

United States Computer Emergency Readiness Team

The 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 coordinate defenses against and responses to cyber attacks across the Nation. The US-CERT provides a 24/7 single point of contact for cyberspace analysis and warning, information sharing, incident response and recovery for a broad range of users, including 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 ICS-CERT operates as a functional element of the US-CERT for cyber incidents related to ICS. 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 mitigate vulnerabilities. This expansion encourages government and private sector participation by reporting and sharing incident and vulnerability information.

Homeland Security Information Network – Critical Sectors

DHS's Homeland Security Information Network-Critical Sectors (HSIN-CS) 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-CS 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-CS Dams Portal, managed by the Dams SSA within IP, provides trusted and vetted public and private sector partners, including owners and operators, 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 MS-ISAC 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 the 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 with local government.

Operating under the auspices of MS-ISAC, the Local Government Cyber Security Committee was established to help identify the cybersecurity challenges facing localities and work toward solutions. This committee, which is voluntary and collaborative, comprises individuals representing towns, counties, cities, and school boards along with 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 efforts to improve the cybersecurity posture of the Dams Sector. In addition, corresponding milestones were established to address the 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, event, or occurrence, as determined by its likelihood and the associated consequences. The three components of risk are threat - 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 - which is a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; and consequences - also known as the effect of an event, incident, or occurrence.

The direct risk challenges include: the threat (those who seek to attack and compromise 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 systems; and how loss of control impacts the interaction with humans, property, and the environment.

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 the optimum security enhancements.

Risk Challenges to Cybersecurity

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

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 exacerbated by the international nature of the Internet and CIKR. An attack could originate from almost anywhere on the planet; CIKR companies often have international partners, suppliers, and customers; and cyber components and systems often have international origins with international maintenance and support. Furthermore, ICS owned and operated by the Dams Sector often include vendors with cyber components and systems with international origins, maintenance and/or support.

Risk assessment and analysis will provide an analytical understanding of this problem. The business case is a subset of risk analysis in that it provides an understanding of the cost benefit of expending resources to reduce risk. Once the problem is recognized and understood through assessment and analysis, it will be possible to design and implement solutions that will act as countermeasures to the system vulnerabilities. Security systems and procedures should be designed and implemented in accordance with standards and accepted industry practices. Training also enables all stakeholders to take proper actions.

A list of challenges regarding the security of control systems were identified and discussed during the Dams Sector Cybersecurity summit and are presented in the tables below.

Milestones For Securing Control Systems

Given the challenges identified, various milestones were identified that could potentially minimize or overcome those challenges. Often these milestones 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 milestones of enhancing training, improving standards, and enhancing capabilities, and the development and use of risk analysis, respectively. A brief summary of milestone development followed by a graphical depiction of the challenges and milestones for each goal are presented below.

Goal 1 - Measure And Assess Security Posture

Goal 1 aims for companies and operational entities to have a thorough understanding of their current security posture in order to determine where control system vulnerabilities exist and what actions may be required to address them. The roadmap envisions that within 10 years the sector will help ensure that owners and operators have the ability and commitment to perform fully automated security state monitoring of their control system networks, with real-time remediation.

Challenges

Currently, asset owners and operators do not have adequate inventories of their critical assets and associated ICS or a good understanding of the risks (threats, vulnerabilities and consequences) of a cyber attack. The growing number of nodes and access points has made identifying vulnerabilities more complex. Widely accepted industry standards, consistent metrics, and reliable measuring tools are not readily available; however, they are essential to assessing the security/risk of these increasingly complex control systems and all of their components and links.

Quantifying risk is a necessary component of risk assessments and for subsequent investment analysis. In addition, cyber and IT systems are inherently dynamic in nature and, as ICS are increasingly more complex, there are few historical experiences from which to make future projection and/or estimates. All of these factors make it difficult to assess the security posture of the sector as well as individual facilities. Furthermore, the physical and electronic isolation of many dam facilities increases the difficulty of understanding full threat and vulnerability parameters; even when known, they are often hard to demonstrate and quantify in terms that are meaningful for decision makers.

Milestones

Near Term

Near-term milestones focus on the establishment of common metrics for benchmarking ICS risk in the Dams Sector; the development of risk assessment tools for measuring ICS risk; the integration of security into operation plans; and the dissemination of accepted ICS standards and guidelines that enable the tools and metrics to be effectively deployed.

Mid Term

Mid-term goals involve the implementation and use of assessment tools in ICS and the development of real-time security assessment capabilities for new and legacy systems. They also call for sector-wide dissemination of training programs and recommended guidelines, such as the Cyber Security Evaluation Tool (CSET) developed by DHS, which assist asset owners and operators in performing self-assessments against cybersecurity vulnerabilities. However, most facilities still require guidance and support to use these tools.

Long Term

The long-term milestone associated with this goal helps to institutionalize the practice of ICS risk assessment with the development and implementation of fully automated security state monitors and response systems in most ICS networks, and the practice of actively measuring performance and benchmarking with other sectors.

Goal 1: Measure and Assess Security Posture

Challenges

Understanding Risk

- Inventory of critical assets, their associated ICSs, and the risk of cyber attack 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
- A cyber attack 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 are necessary but not available to measure and assess security status
- 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 understanding 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

Mid Term (2-5 years)

- Implementation of training programs throughout the Dams Sector on the control system security recommended guidelines
- 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 fully automated security state monitors in most dam control systems networks
- Industry-wide active assessment of ICS security profiles including benchmarks against other sectors

Goal 2 - Develop And Integrate Protective Measures

As security problems are identified and security postures assessed, Goal 2 calls for known protective measures to be applied and new solutions developed to reduce system vulnerabilities, system threats, and their consequences. The sector aspires to develop policy and technology solutions for new and existing systems on an ongoing basis to meet emerging needs. For legacy systems, protective measures often include the application of proven 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. As these legacy systems age, they will be replaced or upgraded with next-generation control system components and architectures that offer built-in end-to-end security. The roadmap envisions that within 10 years asset owners and operators will be using ICS that have been upgraded to incorporate state of the art protection measures commeasure to risk.

Challenges

The development and implementation of effective protective measures face several challenges. Today's control systems are increasingly interconnected and operate on open software platforms. Communication between remote devices and control centers and between business systems and control systems is a common security concern vulnerability that requires secure links, device-to-device authentication, and effective protocols. Many ICS have poorly designed connections between control systems and enterprise networks use unauthenticated command and control data, and do not use adequate access control for remote access points. In some cases, access control capability is available for ICS, however, may not be enabled or implemented properly (e.g., using default vendor passwords or sharing passwords). In addition, 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.

Milestones

Near Term

Near-term milestones for this goal involve the development of control system protection guidelines that assist in ensuring existing access controls are properly implemented and enabled. These guidelines should be disseminated widely within the Dams Sector, along with additional training materials regarding cyber and physical security for control systems. Also during this time, mechanisms should be established for sharing information between asset owners and operators and vendors to develop improved protection tools. Lastly, security patches for common vulnerabilities should be developed and widely distributed among asset owners and operators.

Mid Term

Mid-term milestones focus on the implementation of new protective tools as well as securing the interfaces between ICS and business systems. This includes securing connections between remote access points and control centers as well as evaluating authorized access to VPN environments. The milestones also call for training programs to support proper use and protocol for these new tools and systems. Training courses for asset owners and operators should continuously be developed and updated to help increase awareness and facilitate culture shifts in ICS security practices. Since each control system is unique, the sector should identify, publish, and disseminate best practices regarding control system security, including securing connectivity with business networks and for providing physical and cybersecurity for remote facilities.

Long Term

The long-term milestone for Goal 2 focuses on securing the integration of ICS and business systems, as well as the installation of cyber resilient ICS architectures that have built-in security and use systems and components that are secure-by-design.

Goal 2: Develop and Integrate Protective Measures

Challenges

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

- There is widespread and continuous connectivity of IT and ICSs, and 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 open communication environments
- Existing ICSs have numerous access points, use default vendor accounts/passwords/ shared passwords, and have poor firewall implementation
- Many ICSs operate using unauthenticated command and control data
- Basic security features are often not enabled on ICS
- The complexity of ICSs increases exponentially with an increase in the number of nodes.
- The use of COTS greatly increases the risk of an ICS

Legacy Upgrade and Patch Management Issues

- The unavailability of patch management that conforms to a 24/7 operating environment with extended vulnerability windows and without regularly scheduled maintenance opportunities
- Older operating platform (legacy and hybrid) systems may have limited or no vendor support, thus limiting their ability to secure the system
- Security upgrades are hard to retrofit to legacy ICSs, may be costly, and may degrade system performance, thus lessening incentives to upgrade those systems

Milestones

Near Term (0-2 years)

- Development of control system protection guidelines for existing ICS
- Enablement of existing ICS access controls throughout the Dams Sector
- Development and implementation of security patches for legacy systems
- Establishment of mechanisms to enhance information sharing between asset owners and operators and vendors
- Identification and dissemination of best ICS security practices among Dams Sector stakeholders
- 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 ICS and business systems
- Identification, publication, and dissemination of best practices, including ones for securing connectivity with business networks and for providing physical and cybersecurity for remote facilities
- Development of high-performance, secure communications for legacy systems

Long Term (5-10 years)

- Secure integration of ICS and business systems

Goal 3 - Detect Intrusion And Implement Response Strategies

Cyber intrusion tools are becoming increasingly sophisticated such that it is impossible to protect ICS from all cyber threats. Goal 3 focuses on the sector's resilience in the face of a successful attack. Resilience requires that facilities have the ability to monitor system integrity and detect intrusions with sophisticated alarming tools. It also requires the capacity to analyze anomalies and manage security events and response strategies. Finally, it requires automated incident reporting processes that include complete audit trails. Within 10 years, it is envisioned that the Dams Sector will be operating networks that automatically provide contingency and remedial actions in response to attempted intrusions.

Challenges

Due to concerns regarding proprietary information, asset owners and operators often do not share information beyond the company regarding past security events and their consequences. In addition, companies do not regularly review security logs. The failure to review and share lessons learned limits response capability in an emergency, even when appropriate security measures are available.

Another major challenge to implementing response strategies is that some measures taken to increase ICS protection may inhibit the capacity to implement quick response strategies in emergencies. For example, in an emergency an operator may need to access control programs in order to mitigate damages and bring the system back on. However, increased access controls could prevent the person most able to fix the system from logging in.

Milestones

Goal 3 requires provisions to detect and respond to the attacks that manage to defeat the protective measures of Goal 2.The milestones for Goal 3 are therefore directed towards ICS incident handling, including detection, response, and recovery from an all-hazards perspective.

Near Term

In the near-term, security features already built into control systems should be identified and enabled as appropriate. Cyber incident response and recovery plans should be developed and incorporated into well-established emergency operating plans. Dams Sector members should also focus on identifying best practices and approved guidelines for incident reporting as well as improved methods for information sharing. In the near-term, asset owners and operators should also be engaging employees in proper training on incident response procedures and begin working with vendors on specifications for new detection and response tools for ICS systems.

Mid Term

By the mid-term, new and improved detection, response and recovery tools with greater effectiveness should be developed. Examples include: intrusion detection systems that perform complete audit trails and automated reporting; tools that help visualize data and communication patterns for identifying anomalies and correlate suspicious patterns with potential threats; and tools for security event management which helps prioritize corrective actions through alarming, trending, forensics, and audits.

In addition, emergency response plans and training procedures should be updated to reflect changes in new tools and best practices. Employee training programs should be conducted to ensure correct implementation of new ICS tools and procedures. Assets owners and operators may also want to develop public communication strategies such as providing public safety training literature on consequences of a disruption from a cyber event.

Long Term

Widespread implementation and use of automated self-healing control system architectures is a major long-term milestone. Within ten years, ICS detection and response tools should have the capability of performing real-time detection and response and should develop control system security certification programs for operators.

Goal 3: Detect Intrusion and Implement Response Strategies

Challenges

- Periodic and appropriate reviews of security logs and change management documentation often receive limited, if any, attention
- Cybersecurity protection measures can negatively impact ability to rapidly respond to emergencies
- It is difficult to keep up with the continuous increase in the sophistication and availability of hacker’s tools and resources

Milestones

Near Term (0-2 years)

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

Mid Term (2-5 years)

- Implementation of intrusion detection software in monitoring sector ICSs, publication of related best practices and guidelines and provision of related training
- Implementation of training programs for new intrusion detection software and any associated updates to response, identification and reporting procedures
- Development of control systems simulators to perform the operator training
- Development of training for control room operators in identifying and reporting unusual events, breaches, and anomalies from a cyber event
- Implement configuration management procedures and test beds for patch installations
- Development of public communication strategies and dissemination of public safety training literature on consequences of a disruption from a cyber event

Long Term (5-10 years)

- Development and installation of self-healing control system architecture throughout Dams Sector
- Implementation of real-time intrusion detection and prevention systems
- Development of control systems security certification program for operators

Goal 4 - Sustain Security Improvements

Goal 4 focuses on sustaining the progress made to improve the protection and response capability of asset owners and operators. Maintaining aggressive and proactive cybersecurity of ICS 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 a sustained advancement in securing their ICS.

Challenges

Information sharing between members of the Dams Sector and other stakeholders is essential for sustaining security improvements; however, it is limited due to uncertainty on how information regarding control system security (including information on new threat developments and best security practices) will be used, disseminated, and protected.

The lack of a strong business case for cybersecurity is also a challenge to many of the roadmap goals, particularly to sustaining security improvements over the longer term. ICS is not traditionally viewed as a part of IT in many business models, and therefore may not be viewed as having value-added benefits to a facility. This challenge is exacerbated by the inherent difficulties in developing cost-benefit analyses models, especially the quantification of business risk in financial terms. Cyber systems are dynamic and there is no long-term experience to project valid attack rate estimates.

Outside of the control system community, there is a poor understanding of cybersecurity problems. In the past, this has translated to a lack of executive level buy-in and support for security investments and minimal public and private investment, interest, and focus on these critical issues.

Milestones

Sustainability of secure control systems in the Dams Sector will be accomplished with strong leadership and commitment that includes long-term partnerships, forums for collaboration, and tools for centralizing information gathering and sharing across the sector. The collaboration and information sharing needs to be applied toward maintaining a cycle of continuous improvement. This cycle includes the institutionalization of cybersecurity such that the ongoing monitoring and upgrading of cyber assets and ICS is a standard operating procedure for owners and operators.

Near Term

In the near-term, the Dams Sector should focus on developing mechanisms for securely sharing information within the Dams Sector and across sectors. A secure forum for information exchange will enable the Dams Sector to more efficiently accomplish the milestones corresponding to each of the goals over the next ten years, and will serve to build the foundation for maintaining ICS security in the future.

Once mechanisms for securely sharing information have been established, industry-wide standards and best practices regarding ICS risk assessment, security tools, procedures and training programs should be disseminated among stakeholders across the sector and updated when deem necessary.

Another important action to accomplish in the near-term is increasing awareness on cybersecurity issues and their implications throughout the sector and across sectors, in order to gain the attention, buy-in and commitment from key stakeholders, including asset owners and operators. Over time, cybersecurity awareness, outreach, training and education programs should be integrated into Dams Sector operations.

Mid Term

In the mid-term, the sector needs to establish a lifecycle investment framework for cybersecurity that accurately depicts the business case for voluntary sector-wide implementation of ICS security measures. This includes using the risk assessment tools developed in Goal 1 to perform cost-benefit-analyses. To address the issue of the sector's investment in control systems, this roadmap advocates for the mid-term development of incentives to accelerate investment in secure ICS. Incentives could also be developed for implementing best security practices and performing regular security upgrades.

Long Term

The long-term milestones focus on widespread adoption of best practices such that it becomes standard procedure to monitor new threats and perform regular upgrades to stay ahead of them. In addition, universities, colleges, vendors, owners and operators are expected to develop education and training programs to maintain a high level of professional cybersecurity expertise within the sector.

Goal 4: Sustain Security Improvements

Challenges

Information-Sharing Issues

- Lack of necessary and constructive relationships with governmental authorities for sharing threat information for the sector
- 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) increases the difficulty and incentives to implement cybersecurity measures
- Funding of activities (e.g. R&D) important to ICS security depends on input from industry to properly 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 and appropriate reviews of security logs and change management documentation often receive 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 cyber attackers

Milestones

Near Term (0-2 years)

- Widespread security awareness among sector, cross-sector, government, industry partners and 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 life cycle investment framework for cybersecurity that can be tailored to the Dams Sector and its members
- Formation of partnerships between government and industry 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, including performing regular upgrades and monitoring new threats across the sector

Goal 5 - Secure-By-Design

Goal 5, also concerned with sustainability and continuous improvement, 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 ICS, will be available and used across the Dams Sector.

Challenges

Currently, the return on investment for vendors to sustain control system and security tool improvement, including R&D to advance the technology, is unclear. Vendors currently do not have adequate requirements or standards to design, build, and maintain cybersecurity into ICS. Evolving cyber threats, changes in cyber-intrusion technologies, and developments in IT can pose challenges to building security into ICS with long lifecycles.

Milestones

Goal 5 requires a new design approach and business model in which vendors and asset owners and operators collaborate on security requirements of ICS, such that protective measures are built into ICS. In addition, it requires that these built-in protective measures take account of the total lifecycle of the ICS product so they can anticipate and accommodate future vulnerabilities and needs.

Near Term

In the near-term, partnerships between vendors and asset owners and operators should be developed and/or enhanced if already established. As the business case for cybersecurity is built and buy-in from executive level management achieved (milestone for Goal 4), owners and operators, in coordination with the R&D community, should work with vendors to collaborate on improvements to built-in security, as well as specify secure-by-design requirements when procuring new systems. The R&D community will also be engaged by increasing awareness of importance of ICS cyber-security.

Mid Term

This roadmap anticipates that next generation ICS with built-in-security will become available in the mid-term. Security will be incorporated into the life cycle of ICS as vendors begin to perceive a viable market for such enhancements. The level of security built into ICS (i.e. how much a particular system is designed to accommodate and adapt to future changes in cyber-security) will vary among asset owners and operators depending on each company's unique business case for the value of such security enhancements.

Long Term

In the long-term, ICS products with built-in security that can accommodate future changes in cybersecurity issues will be produced at commercial scale. R&D projects on next generation systems will be widespread and continually using feedback from vendors and ICS end-users to make improvements.

Goal 5: Secure By Design

Challenges

- The increasing use of standardized ICSs technology and posture increases attack opportunity
- Enhanced cybersecurity upgrades on ICSs with long design lives that were not initially designed for current cybersecurity requirements may be difficult 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
- Lack of incentives for vendors implement and sustain secure-by-design enhancements to their ICS products

Milestones

Near Term (0-2 years)

- Development of partnership 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 systems vendors and the research and development community; and development of guidance documents and training materials.

The Dams Sector will pursue a focused, coordinated approach that aligns current activities to roadmap goals and milestones; initiate specific projects to address critical gaps; and provide 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. They specifically avoid calling for regulation that would impose these priorities and actions on owners, operators and vendors.

As a result of continuing cyber attacks against critical infrastructure, it is envisioned that ICS security enhancements will be incorporated into the life cycle of the systems 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 the 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 extremely high impact costs. This 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, and to help sustain the efforts of this roadmap, the risk management planning process must include constant exploration of emerging ICS security capabilities, vulnerabilities, consequences and threats.

This roadmap encourages organizations to participate in ways that will best capitalize on their distinct skills, capabilities, and resources for improving the security of ICS.

This affords companies and organizations the flexibility to pursue projects that correspond with 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 the ability to recognize cyber incidents when they occur and respond to them effectively using the most reliable mitigations 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, have 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 of the facility or ownership characteristics.

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 to thwart cyber attacks 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 regards 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 ICS.

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 ICS.

Implementation Framework

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

Socialization

The first phase of 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 identifying roles and delegating responsibilities. It is the time to leverage the buy-in from key players and to motivate industry leaders to step forward and become more actively involved. A critical component for 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 and forward movement from the socialization process.

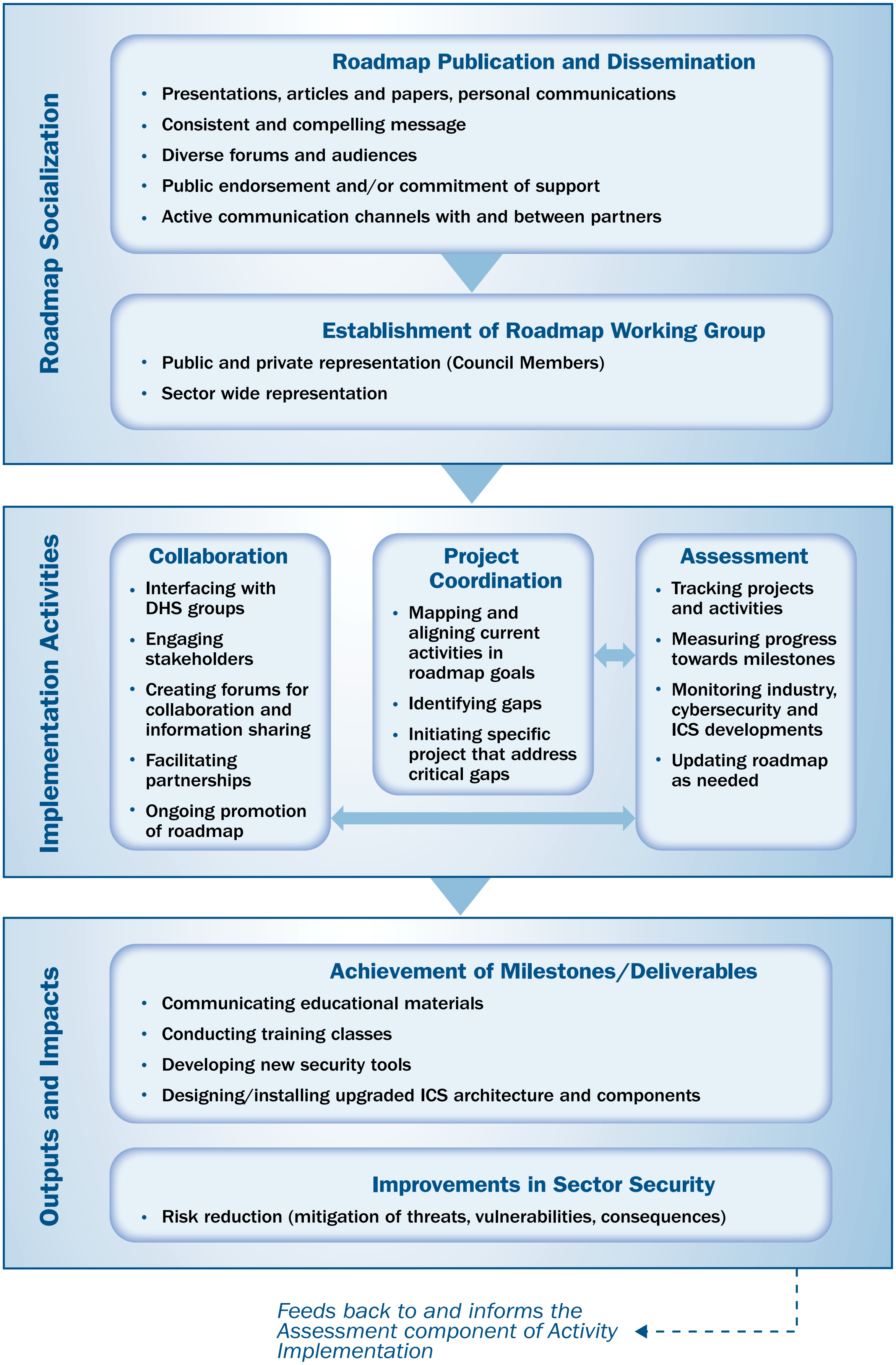
Implementation Activities

The second phase is where the majority of the milestones, including policy development, partnership formation, training initiatives and R&D efforts are implemented. The working group will serve as the mechanism for the project coordination of roadmap activities and takes 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.

Figure 3: Roadmap Implementation Process



Roadmap Socialization

Roadmap Publication and Dissemination

- Presentations, articles and papers, 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
- Ongoing promotion of roadmap

Project Coordination

- Mapping and aligning current activities in roadmap goals
- Identifying gaps
- Initiating specific project 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
- Conducting training classes
- Developing new security tools
- Designing/installing upgraded ICS architecture and components

Improvements in Sector Security

- Risk reduction (mitigation of threats, vulnerabilities, consequences)

Feeds back to and informs the Assessment component of Activity Implementation

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 overtime in meeting roadmap milestones.

Assessment

Project assessment involves the assessment and feedback of roadmap activities and ensures they remain on target. In addition, it entails the assessment of industry developments in ICS and IT and evolving security threats that may affect roadmap activities and require the readjustments of goals, milestones, and activities. As the workgroup tracks these changes, it may call for a revision of 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 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 education materials, documentation of best practices, Web sites for information sharing, new security patches and tools, and upgraded ICS architecture and components in phase three. The concrete outputs and deliverables generated from the roadmap activities are deployed, primarily by owners and operators, and results 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 linear 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 protection 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
- Self-certification program

As such, it is intended to guide the planning and implementation of collaborative cybersecurity programs that 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 spans all CIKR 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 CIKR.

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 CIKR protection 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; and
  - – 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 protective measures implemented by infrastructure owners and operators; and
  - Support international efforts to strengthen the protection of CIKR.
- State, local, tribal, and territorial governments:
  - Supplement DHS protective security guidance with additional knowledge from the State/local level to the private sector within their communities; and
  - Provide National Guard, State, and local law enforcement personnel and 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 the 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 protective 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/; and
  - 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; and
  - Support Research & Development activities.

Guiding And Aligning Existing Efforts

As discussed in Chapter 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 the Critical Infrastructure Partnership Advisory Council	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 National Cyber Security Division, 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

Activity	Lead Organization	Scope	Major Actions and Events
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 tests 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 • Certification Program Operational – Planned May 2009

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. Blair, Dennis C., Director of National Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, 12 February 2009, (**http://www.dni.gov/testimonies/20090212_testimony.pdf**).
3. Brennan, John, Assistant to the President for Homeland Security and Counterterrorism, (**http://www.whitehouse.gov/blog/09/03/02/Cyber-review-underway**).
4. Chemical Sector Roadmap Working Group, Roadmap to Secure Control Systems in the Chemical Sector, September 2009, (**http://www.us-cert.gov/control_systems/pdf/ChemSec_Roadmap.pdf**).
5. Federal Energy Regulatory Commission, FERC approves new reliability standards for cybersecurity, January 17, 2008 (**http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp**).
6. Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure, Order No. 706, 2008 (**http://www.ferc.gov/whats-new/commmeet/2008/011708/e-2.pdf**).
7. Florida Reliability Coordinating Council, Reliability Standards Development Bulletin, January 2008,(**https://www.frcc.com/Standards/Shared%20Documents/FRCC%20Reliability%20Standards%20Development%20Bulletin-%20January%202008.pdf**).
8. Multi-State Information Sharing and Analysis Center (MS-ISAC), About the MS-ISAC, (**http://www.msisac.org/about/**).
9. North America Electric Reliability Corporation, Reliability Standards, 2009, (**http://www.nerc.com/page.php?cid=2|20**).
10. Northwest Hydroelectric Association, Dam Safety and Security, 2008, (**http://www.nwhydro.org/resources/laws_regulations/dam_safety_security.htm**).
11. Purdue University, Barack Obama's speech at the University of Purdue, July 16, 2008, (**http://www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.htm**).
12. 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**).
13. 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**).
14. Stouffer, Keith, et al., Final Public Draft, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST), Special Publication 800-82, September 29, 2008, (**http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf**).
15. Turner, Aaron R., Idaho National Laboratory, 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,

April 19, 2007, (**http://homeland.house.gov/sitedocuments/20070419153130-95132.pdf**).

16. 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**).
17. U.S. Department of Homeland Security, National Infrastructure Protection Plan, 2009, (**http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf**).
18. U.S. Department of Homeland Security, Written Statement of Donald (Andy) Purdy, Jr. Director (Acting), National Cyber Security Division, July 19, 2005, (**http://hsgac.senate.gov/public/_files/PurdyTestimony.pdf**).
19. U.S. Department of Homeland Security, Control Systems Security Program (CSSP), (**http://www.us-cert.gov/control_systems/**).
20. U.S. Department of Homeland Security, Control Systems Security Program (CSSP), Cyber Threat Source Descriptions, (**http://www.us-cert.gov/control_systems/csthreats.html**).
21. U.S. Department of Homeland Security, Control Systems Security Program (CSSP), Overview of Cyber Vulnerabilities, (**http://www.us-cert.gov/control_systems/csvuls.html**).
22. 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/**).
23. U.S. Department of Homeland Security, Office of Infrastructure Protection, Dams Sector Branch, National Infrastructure Protection Plan - Dams Sector, 2008, (**http://www.dhs.gov/xlibrary/assets/nipp_snapshot_dams.pdf**).
24. U.S. Department of Homeland Security, Triennial Rewrite and Reissue of the 2010 Sector-Specific Plans-Guidance for Sector-Specific Agencies, 2009.
25. U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team (US-CERT), US-CERT – About Us, (**http://www.us-cert.gov/aboutus.html**).
26. U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team (US-CERT), US-CERT – Cyber Threat Source Descriptions, (**http://www.us-cert.gov/control_systems/csthreats.html**).
27. U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team (US-CERT), US-CERT – Overview of Cyber Vulnerabilities, (**http://www.us-cert.gov/control_systems/csvuls.html**).
28. U.S. Department of Energy, Roadmap to Secure Control Systems in the Energy Sector, January 2006 (**http://www.controlsystemsroadmap.net/pdfs/roadmap.pdf**).
29. 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**).
30. U.S. Senate, Cybersec.4, Staff Working Draft, March 2009 (**http://cdt.org/security/CYBERSEC4.pdf**)
31. Water Sector Coordinating Council Cyber Security Working Group, Roadmap to Secure Control Systems in the Water Sector, March 2008, (**http://www.nawc.org/policy-issues/utility-security-resources/Final%20Water%20Security%20Roadmap%20 03-19-08.pdf**).
32. Weiss, Joseph M., Control Systems Cybersecurity - The Need for Appropriate Regulations to Assure the Cyber Security 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
ASI	Advanced Systems Institute
ANL	Argonne National Laboratory
ANSI	American National Standards Institute
BCIT	British Columbia Institute of Technology
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISSP	Certified Information Security Professional
COTS	Commercial off-the-shelf
CPU	Central processing unit
CSCSWG	Cross Sector Cybersecurity Working Group
CSSP	Control Systems Security Program
DCS	Distributed Control System
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
ERO	Electric Reliability Organization
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
GCC	Government Coordinating Council
HMI	Human Machine Interface
HSIN-CS	Homeland Security Information Sharing Network-Critical Sectors
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
IEEE	Institute of Electrical and Electronic Engineers
INL	Idaho National Laboratory
I/O	Input/output interface system
ISA	International Society of Automation
IT	Information Technology
LAN	Local Area Network
LGCC	Levee Sub-Sector Government Coordinating Council
LSCC	Levee Sub-Sector Coordinating Council
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Corporation

NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NSTB	National SCADA Test Bed
PC	Personal Computer
PCS	Process Control System
PCSRF	Process Control Security Requirements Forum
PDA	Personal Digital Assistant
PLC	Programmable Logic Controller
Reclamation	U.S. Bureau of Reclamation
RTU	Remote Terminal Unit
SANS	SysAdmin, Audit, Network, Security Institute
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SSA	Sector-Specific Agency
SSP	Sector Specific Plan
USACE	U.S. Army Corps of Engineers
US-CERT	United States Computer Emergency Readiness Team
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.

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 refer to commercially available technological components and systems, including both hardware and software.

Control System. A CS is a device or group of devices that 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, and 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.

Process Control Systems. Descriptive of systems in which computers or intelligent electronic devices are used for automatic regulation of operations or processes. Typical are operations wherein 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 wireless high-speed Internet and network connections. 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."

According to the 2009 Annual Threat Assessment, nation states and criminals are targeting government and private sector information networks within the US to gain competitive advantage in the commercial sector.[d] A successful cyber attack against a major financial service provider could severely impact the national economy, while cyber attacks 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, and 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 directives and laws. In 1998 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 later 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.

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

[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/testimonies/20090212_testimony.pdf.**

[e] **http://www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.html.**

[f] U.S. Senate, March 2009, Cybersec.4, Staff Working Draft, **http://cdt.org/security/CYBERSEC4.pdf.**

Federal Information Security Management Act of 2002 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 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 CIKR.

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 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 in those sites."

In late 2003, the President issued Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," to implement Federal policies. HSPD-7 outlined how government will coordinate for critical infrastructure protection and assigned DHS the task of coordinating critical infrastructure protection, including physical and cybersecurity, for 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, appointed by the President, who are selected from the private sector, academia, and state and local government, representing senior executive leadership expertise from the critical infrastructure and key resource 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 to improve the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, to protective strategies and clarification on roles and responsibilities between public and private sectors.

The *National Infrastructure Protection Plan* was issued in 2006. It establishes a partnership model for collaboration, consisting of a Sector Coordinating Council and a Government Coordinating Council for each sector, as applicable and consistent 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, 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 CIKR sectors as well as with DHS, Federal Energy Regulatory Commission (FERC), and other government agencies, including the Dams Government Coordinating Council.

The Dams GCC acts as the government counterpart and partner to the SCC to plan, implement, and execute sector-wide security programs for the sector's assets. It comprises representatives from across 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.

Members of the Dams Sector Councils collaborated with DHS to develop the 2007 and 2010 *Dams Sector-Specific Plan (SSP)*. The 2010 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 directed towards cybersecurity as well as 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 mission. These systems provide the capability for remote control and monitoring of the operation from a centralized control center, through various modes of communication, technologies and methods.

Dam operations are controlled either on-site or remotely, and may rely to some extent on ICS for operation or monitoring purposes. ICS 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 for processing in 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 ICS may also automatically take some corrective actions without the interaction of the staff.

ICS designs and implementations vary from project to project, owing 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 with its own design of hardware and software programming.

Dams, especially those located upstream of population centers, 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 cyber attack 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 in those systems where security measures were not included in the original design.

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 dam, the ICS is also known as a Supervisory Control And Data Acquisition (SCADA) system. The term SCADA usually refers to centralized systems, which 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 by 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 sub-system 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.

An RTU is a microprocessor-controlled electronic device that interfaces objects in the physical world to 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 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 depending on the flow of water through part of an hydropower production process and the needed power output; however the SCADA (ICS) system may allow operators to change the set points for the flow, 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 for automated real-time data collection and analysis, of inflows, outflows, gate openings, position sensors and water elevations.

Existing ICS in the Dams Sector vary widely based on the age and generation of the system; thus, they also vary with respect to complexity and sophistication. Some ICS are closed and use isolated networks as well as proprietary communications protocols. Other ICS 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 electric power grid. Most dam owners, if not all, use various computer security methods for master terminal units, data servers, and historians, such as authentication procedures, encryption, firewalls, anti-virus software, and anti-spyware.

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 covers, the more sophisticated the ICS becomes. Furthermore, the amount of automation of the system combined with the amount of built-in redundancy will create a more elaborate system.

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

ICS for water supply systems are used to control and monitor remote operations of penstocks, spillway gates, control water level in reservoirs, and provide seasonal weather data using the common control system network. Due to the primary mission to meet the water needs of the local population, a water supply facility is normally tightly coupled 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 ICS 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 on the same ICS communication networks utilizing the same 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 in 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 on the same ICS communication networks and therefore, utilizing the same bandwidth. ICS are also used to obtain data from sensors for water quality issues, 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 the control and communication parts, or a combination of these.

ICS are used to control and monitor electric generating equipment. ICS of power generation is normally more sophisticated than the control of water supply structures. For example, control systems are used to control governors and governor systems, relays, voltage, frequencies, and automatic voltage regulators among others. In the future, there will be more pressure to provide power system stabilizer information from the governor systems, which could lead to increased vulnerability of the 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 the hydropower generation via Ethernet fiber optics. These systems frequently use an unencrypted backbone infrastructure, which connects with RTUs as a gateway to the DCS.

ICS are available through a wide variety of network architectures, including COTS, HMI, data acquisition and control, and monitoring software and hardware. In addition, ICS with proprietary protocols and codes can also be developed and used for specific projects. Usually, ICS 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 ICS using known vendor PLC units to operate hydropower generation plants on an Ethernet LAN from the control center. The power generation equipment uses DCS connected to the above-mentioned ICS. The Master Terminal Unit normally uses a Windows-based operating system and COTS HMI interface. The power generation DCS uses RS232 serial data protocol.

In some cases, power generation projects use separate hard-wired systems as the backup system using an Automatic Generator Control (AGC), prior to going full manual control of generation equipment by the field personnel. The disruption of any command and control to devices in the power generation plant does not impact the 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 are 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.

Projects that have hydropower generation 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, the ICS may have the ability to have a direct communication link to the RTO control center. This communication link can be created via wireless microwave as well as through secure lines using an inter-control center protocol for data (such as voltage, frequency, ampere, power output in MW, etc). It can also be used by the RTO to send requirements to the project production. The communication occurs through a dedicated fiber optics link to the microwave antenna, which includes a firewall on both sides of the communication and encryption to the data.

As a general rule, projects communicate with an RTO for any operational changes via data transmissions over the public switched telephone network. The RTO does not have access to the controls of the hydropower generation equipment and/or field devices. If an incident occurs that forces the project to control the system by manual operation, communication between the projects and the RTO is conducted through a voice system.

Spillway gates are an essential dam component as they are used to control water releases in 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 and ICS that can be either directly connected to or completely separated from other ICS in the project. In the case that 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 the data. Similar to the 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 microwave signal, or the use of specialize networks, such as the Synchronous Optical Network (SONET). SONET is used primarily for backbones composed of fiber optics and performs a complicated timing and multiplexing scheme. 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 creating a single point of failure into the system.

Some projects that remotely monitor and periodically control operations do not have AGC links to the 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 hard-wired and connected to a separate network from the ICS, even though the system may have the capability to interconnect. In other cases, ICS will 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 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 rest of the networks provides a higher level of protection for the project by lowering the amount of access points as well as the amount of direct and indirect connections. By lowering the amount 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 amount 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 exposed to the outside world.

In some projects, maintenance for the ICS and/or its components is commonly outsourced to third party vendors. These vendors can access the ICS 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, fill and empty valves, lock signals, lock lights, interlock safety control features, as well as all of the lock's electrical and mechanical sub-systems. The PLC system usually incorporates a backup control system; it also provides monitoring and reporting of lock equipment status. Control of the lock equipment is initiated by the on-site operators either from a control stand located adjacent to the equipment or from the navigations 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 ICS where technology has been developed for very specific use, the lifetime of the deployed technology is often 15-20 years or longer. The lifecycle of a PLC is much longer than both the operating system (O/S) and the HMI software. Since O/S 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 technology incompatibility. Achieving a comfortable level of security requires non-intrusively retrofitting existing insecure and legacy ICS with new technology. In most cases, it is economically and technically infeasible to retrofit security appliances to the existing control system infrastructure.

Improving the security of legacy ICS against cyber attacks require flexible solutions that are easy to install and do not impact system performance and operations. Development of retrofit solutions that can provide robust cybersecurity to existing fielded ICS has been of particular interest to industry organizations such as NERC, the Gas Technology Institute, and the International Society of Automation. Since ICS typically have useful lives of more than 15 years, retrofit solutions usually play a key role in addressing cybersecurity concerns and bringing fielded systems into compliance; while embedded security features are designed as a part of a more robust ICS in the future. The efforts of the aforementioned organizations are yielding security recommendations, including NERC (CIP-002 through -009) 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 increasing interconnectivity, faster data transmittal, and connecting older systems to newer control systems are the factors increase the level of vulnerability and probability of an incident in an ICS.

Integrating new technologies into these systems is especially difficult, or even impossible in some cases. For example, older versions of operating systems may no longer be supported by the vendor, thereby making some 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 of the patches 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 to create electronic perimeters of security to protect the system, without having to invest in newer, more secure systems. Technologies presently available for the protection of ICS include firewalls, honeypots, antivirus, cryptography, intrusion detection and prevention systems, etc. With these technologies, the security of existing ICS can be significantly enhanced to protect against cyber attacks.

The use of firewalls in the perimeters of ICS is done to prevent unwanted communication passing through the line of communication where the equipment is present. Firewalls, if configured correctly, can effectively prevent an entity that may reside in the corporate network from taking over the control network, or 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 entrance of the system. The main objective of antivirus software is to prevent the attack of 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 a non-comprehensible message, and then back again, to prevent information from being easily understandable 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 ICS 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 without causing disruption to 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 a wide event from occurring throughout the system, a phased-in approach should be utilized when implementing this type of solution; preliminarily across the more vulnerable connections, followed by wider deployment across the entire ICS network.[g]

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; as well as a processor to record the events and create the alerts needed. 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 ICS 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 date can be accessed by whom, as well what operations are allowed to be performed on that data.

When using a combination of the above technologies, ICS are completely separate 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 different 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 the attacker has to 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, thereby 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 are not enough resources to handle manual operation of remote and multiple sites.

A significant vulnerability at some dam project sites can be attributed to the combination of the lack of physical and cybersecurity protective measures, as well as the attitude of "security through obscurity" when it comes to ICS. This concept reflects some operators' belief that security is present based on the outsider's lack of knowledge and

[g] Juan C. Asenjo, 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.**

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 strong enough 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 encryption for data. However, the lack of security at physical locations that provide access to cyber-related components, (e.g., telephone rooms, cables conduits, switch boards, LAN connections close to control centers) makes the project vulnerable to intentional insider attack or from accidental contact.

The task of securing legacy assets from cyber attacks will continue to expand and grow even as newer systems are gradually brought online. At some phase in their service lifetimes, all ICS 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 system.

Generally, the floodgates are left open either for gravity drainage of water or for normal use of navigable waterways. The floodgates are closed to either 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 its 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 that 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 electronically available through the use of specialized weather, water, and environmental data collection systems.

For example, Reclamation uses an agricultural weather information system called "AgriMet," with the purpose of promoting water and energy conservation. AgriMet is a network that 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., amount of water used 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 view-only workstations to sponsors.

Similarly, the HydroMet network system is comprised of communications and computer systems that provide information on water and environmental data that is remotely gathered 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 the 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 ICS 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 monitoring system designed to aid dam operators at hydropower plants in achieving optimum generation. This system allows the monitoring of stream banks saturation (banks slump) and control of generation equipment to curtail generation through the ICS if necessary. The systems could feed information into the ICS as a control line to indicate high levels of generation. Even though the system does not have control capabilities, it functions similarly to a "warning system" to the operators.

Securing Industrial Control Systems in the Dams Sector

Identifying the common access points, interconnections, and critical cyber elements and physical components associated with ICS, 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. Risk analysis is therefore, an important criterion in establishing an effective security policy.

Identification of Critical Functions & 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 the ICS. Identifying critical functions and operations dependent on the ICS should include the following:

- 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" or 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 the 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, who will not compromise 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 electric power systems. The Dams Sector recognizes that the CIP Standards apply to all bulk electric power systems and under these standards, a hydropower generation facility must be considered for applicability of them.

Each dam project function has conflicting security guidance because the majority of assets are identified as "critical" based on the functions provided. This can be seen in hydroelectric generation or navigational locks, both projects have critical assets necessary for their respective operation and missions.

It is recognized that cyber attacks could happen and can 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 reliability, including the ability to restore after a partial or total operational shutdown. Multiple element contingencies without accompanying faults are very probable under this type of threat.

Identification of Common Cyber Access Points

To reduce the probability of a successful cyber attack on Dams Sector ICS, 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 an obvious 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 the facility and inserting it into a PC.
- Malware can also be introduced by simple electronic mail containing some type of media or link to the malicious software. Even though this type of infection is well known, it is still one of the easiest to use and has the highest probability of infection, especially in a large company.
- A new threat that has emerged in the past couple of years is the possibility of a Bluetooth-enabled device (cell phone, camera, laptop PC, or PDA) being infected with a virus and passing that virus to other devices (e.g., a Bluetooth-enabled laptop PC that also has an Ethernet interface) that can bridge the virus onto the control system LAN. This problem becomes more complex as Bluetooth is embedded in more devices, such as printers and scanners. A virus

could be passed to these devices and find its way into a computer that accesses that device.

- Any Wi-Fi enabled computer that also has an Ethernet connection. An attacker could use the Wi-Fi connection to bridge the control system LAN, potentially obtaining the access rights of the owner of the computer via this connectivity.
- A rogue or insufficiently protected Wi-Fi AP (access point), as well as the activation of unnecessary ports in networks where control system reside can both be attacked, although this would give the successful attacker access to the LAN and additional effort 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 path of least resistance since they are designed to have quick access to the control network.

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

There should not be remote access points to any of the power-generating equipment, spillways, and navigation lock network systems provided to vendors and/or other support entities.

Control operators should use a separate Administration LAN or other isolated system for emails and other administrative functions. 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 LAN/WANs must be adequately protected by firewall technology. An insufficiently configured or technically inadequate firewall (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.

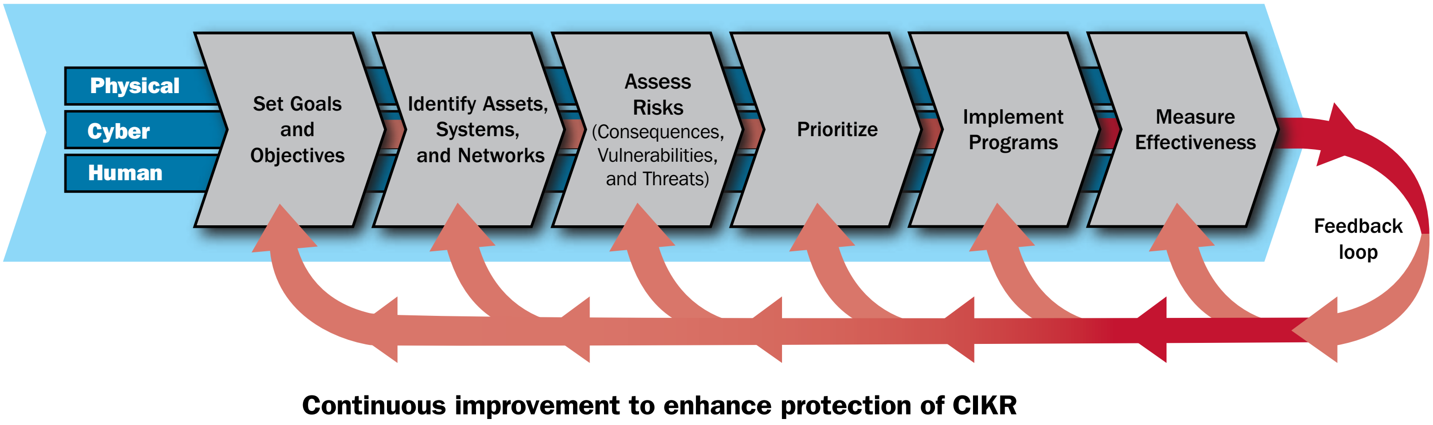
- The most basic vulnerability of a control system is to an insider attack by someone who has physical access to the control system itself. Such an attacker, having first taken steps to damage the restoration media, could go up to the system console and issue commands to delete critical files and applications on both the primary and the backup systems. A system-level programmer or a system administrator with root (administrative) access has essentially unlimited ability to wipe out the software of the operating system, in addition to control system-specific programs and data files.
- Along a similar line, an insider who has operational access rights on the control system (e.g., a senior operator) could issue commands through the operator's console, causing dangerous or destructive control actions (e.g., tripping circuit breakers, closing valves and stopping pumps). This would be even more dangerous if that same attacker had remote operational system access (e.g., remote X-terminal emulation or actual operator console software).
- Just as malware can be introduced into a PC on the control system LAN, the same thing can happen on the corporate LAN/WAN and, if the firewall separating the control system LAN from the corporate WAN isn't adequate, the malware can find its way onto the control system LAN and into the control system computers.
- Just as a Wi-Fi AP can be used by an attacker to break into the control system LAN, the same thing can be done on the corporate LAN/WAN.

Identification of Access Points

- Another access point to the ICS is the point-to-point connections between a control system and another system through a public or private network (possibly a backup control system at an alternative operating site or a regional control center). The use of correctly configured firewalls at every access point, as well as minimizing the number of direct lines between networks is both crucial requirements for the protection of the independent networks.
- ICS use readily available, well-documented legacy, serial communications protocols for interrogating and commanding field-based RTUs. These RTUs are connected by single-frequency licensed radio or leased analog telephone circuits. It has already been proven that a person with a radio, a laptop PC, some commercial software, and reasonable physical proximity can take control of RTUs and override the ICS. Also tapping into a telephone line the attacker can cut the ICS off entirely and control any RTU on that same telephone line.[h]

[h] William T. Shaw, June 1, 2007, SCADA Security: 14 Obvious Points of Attack, Electric Light & Power, **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.**

Figure 4. NIPP Risk Management Framework (Source: NIPP 2009)


Physical
Cyber
Human
Set Goals and Objectives
Identify Assets, Systems, and Networks
Assess Risks (Consequences, Vulnerabilities, and Threats)
Prioritize
Implement Programs
Measure Effectiveness
Feedback loop
Continuous improvement to enhance protection of CIKR

- In a large and geographically distributed corporation, the likelihood that there are unsecured telephone connections to a corporate WAN is probably greater than the likelihood that such connections to the control system exist. However, these telephone connections into the corporate WAN may pose a threat to the control system and provide a path for an attacker to reach the control system, if the control system is interfaced to the corporate WAN at any point.
- Corporate web servers, e-mail servers, and Internet gateways provides access to attackers coming across the Internet. A simple and effective way to defend against this type of attack is the use of honeypots and anti-virus software to detect, deflect, or in some cases counteract attempts at unauthorized entrance of 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 ICS, an important aspect of risk assessment is determining the value of the data that is flowing from the control network to the corporate network, remote operation of critical components, communications systems, etc.

In some situations, the risk may be physical or social rather than purely economic. The risk may result in an unrecoverable consequence rather than a temporary financial setback. Effective risk assessments clearly delineate the mitigation cost compared to the effects of the consequence. An accurate risk assessment of critical cyber assets will assist in providing Dams Sector stakeholders the ability to prioritize security needs and focus limited resources on the most urgent security issues. Risk assessment data is also necessary to 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. The focus should be on those assets, systems, and networks which, if damaged, would result in significant consequences—impacts on national economic security, national public health and safety, public confidence, loss of life, or some combination of these adverse outcomes. The results of this approach should drive Dams Sector risk-reduction and management activities.[i,j]

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 to ubiquitous connectivity and reduction in human oversight in ICS has created significant vulnerabilities in all types of critical infrastructures. Cyber attack tools are increasing in sophistication and ease of use, threatening to outpace security efforts for ICS.

The convergence of ICS with public and private business networks has potentially exposed the ICS to additional security vulnerabilities. Unless appropriate security controls are deployed within and throughout the business and ICS network, cybersecurity breaches in business system security may affect the integrity and the operations of Dams Sector ICS.

[i] DHS, 2009, National Infrastructure Protection Plan: 2009

[j] DHS, 2009, Triennial Rewrite and Reissue of the 2010 Sector-Specific Plans-Guidance for Sector-Specific Agencies

The U.S. Department of Energy's National SCADA Test Bed program has funded 12 separate control systems security reviews, during which experts from Idaho National Laboratory have found that all of the evaluated systems suffer from high-impact security vulnerabilities that could be exploitable by a low-skill-level 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 in currently deployed systems, enhanced security controls cannot easily be implemented 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. Additionally, 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 different 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 as 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 that follow the path of least resistance, which could lead them to the ICS that underlie our critical infrastructures. Information security experts agree that without implementing risk mitigations, ICS will continue to be vulnerable.

Based on historical and current trends of cybersecurity incidents in other technology domains, the corrections will most likely begin with small-scale incidents focused on economic gain, followed by the release of publicly available vulnerability discovery tools, and then a transition to large-scale incidents designed to reduce confidence in the infrastructure systems themselves.[k]

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 internet and open digital communication, the threat to dams today can come from cyber attack on ICS that monitor and control essential elements of the dam operations. Developing a clear understanding of threats is a fundamental element of vulnerability assessments 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 ICS refer to persons who attempt unauthorized access to ICS device and/or network 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 paths. Threats to Dams Sector ICS can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders as follows:

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- Insiders
- Phishers
- Spammers
- Spyware/malware authors[l]

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 CIKR 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.

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 policy and procedures lead to mitigation techniques designed to thwart attacks, managing the risk to eliminate or minimize the consequences. The degradation of dam

[k] Aaron R. Turner, April 19, 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, Idaho National Laboratory, **http://homeland.house.gov/sitedocuments/20070419153130-95132.pdf..**

[l] US-CERT, 2009, Cyber Threat Source Descriptions, **http://www.us-cert.gov/control_systems/csthreats.html.**

operations, economic status, or national confidence could all justify mitigation. The fiscal justification for mitigation has to be derived by the cost-benefit compared to the effects of the consequence that should include 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, long-term costs due to environmental damage);
- **Psychological:** Effect on public morale and confidence in national economic and political institutions (encompassing changes in perception emerging after a significant incident that affects the public's sense of safety and well being and can manifest in aberrant behavior);
- **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 cyber attack from inside and outside the control system network. To understand the vulnerabilities associated with ICS, sector owners/operators should review the types of communications and operations associated with the control system as well as have an understanding of how the attackers are using the system vulnerabilities to their advantage. It is recommended that understanding control system cyber vulnerabilities should include the following analysis:

- Access to the Control System LAN
- Common Network Architectures
- Dial-up Access to the 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 the Data Acquisition Equipment
- Exporting the HMI Screen
- Changing the Database
- Man-in-the-Middle Attacks[m]

Approaches for Prioritizing Critical Cyber Elements

The NIPP provides a methodical approach for risk analysis and management (Figure 4) that establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector risk and can be readily applied as an approach to prioritize critical cyber and ICS elements of the Dams Sector. The risk management framework is structured to promote continuous improvement to overall sector protection by focusing activities on efforts to: set goals and objectives; identify assets, systems, and networks; assess risk based on consequences, vulnerabilities, and threats; establish priorities based on risk assessments and increasingly, on return-on-investment for mitigating risk; implement protective programs and resilience strategies; and measure effectiveness.

Summary of Sector Challenges and Development

Cost/Benefit Analysis

Developing and integrating security advances into ICS architectures can be extremely costly. 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 cyber attack. Without sufficient means to fully quantify and demonstrate the potential impacts of cyber attacks on Dams Sector ICS, 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 existing and

[m] US-CERT, 2009, Overview of Cyber Vulnerabilities, **http://www.us-cert.gov/control_systems/csvuls.html.**

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 ICS security effort is based upon three guiding principles. These principles are: Protect, Detect, and Respond. These can be more completely defined as follows:

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

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 is effectively no protection provided. No single security measure itself is foolproof as vulnerabilities and weaknesses could be identified at any point in time. In order to reduce these risks, implementing multiple protection measures in series avoids single points of failure.

In order to safeguard the process control system from electronic attacks (e.g. hackers, worms and viruses), it may be insufficient to rely on a single firewall, designed to protect the corporate IT network. A much more effective security model for ICS is to build on the benefits of the corporate firewall with an additional dedicated process control firewall and deploy other protection measures such as anti-virus software and intrusion detection. Such a multi-layer security model is referred to as *Defense in Depth*.

When implementing security measures, there is a natural 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, but considerations must also be given to associated procedural and managerial requirements.

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

Research & Development Needs and Considerations

One of the Dams Sector goals in this effort is to identify the R&D security technology needs, priorities, and achievements, in order to enhance and sustain ICS security and resilience. R&D serves to improve cybersecurity protective capabilities or dramatically lowers the costs of existing capabilities so that State, local, tribal, territorial, and private sector partners can afford to do more with their 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-specified patch testing protocols;
- Development of intrusion detection and intrusion protection systems, leveraging efforts currently underway in the I3P program;
- Opportunities for 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 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.

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 the optimum security enhancements. Several examples of these challenges are as follows:

- A lack of developed business cases for control system security.
- A lack of clear and specific up-front security requirements.
- Limited understanding of cybersecurity risks.
- Rapid change in threat actors and vulnerabilities.
- Limited resources to mitigate risks.
- Difficulty or impossibility of integrating new technologies into legacy systems in some cases.
- Issues with managing changes in an organization's mission.
- Differing viewpoints of priorities within the sector.
- Difficulty in fully implementing 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 the opportunities to mitigate an incident through human oversight.

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

A significant piece of this challenge is the ability of owners/operators to make risk management decisions, including those for cybersecurity, based on the 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 the roadmap is to encourage Dams Sector stakeholders to develop a set of milestones, challenges to achieve the milestones, and potential solutions to overcome the barriers regarding cybersecurity. This roadmap should be further developed to help identify sector challenges and opportunities to secure ICS. To enhance information sharing and partnership, the developed roadmap needs to be publicized and easily accessible.

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 projects.

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 with 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 how the results will contribute to addressing particular challenges in the roadmap, identify gaps, and coordinate 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 could later be developed in a technical plan, as appropriate. 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.

Appendix D: Roadmap Milestones

Near Term (0-2 years)

Goal 1: Measure and Assess Security Posture

- 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

Goal 2: Develop and Integrate Protective Measures

- Development of control system protection guidelines for existing ICS
- Enablement of existing ICS access controls throughout the Dams Sector
- Development and implementation of security patches for legacy systems
- Establishment of mechanisms to enhance information sharing between asset owners and operators and vendors
- Identification and dissemination of best ICS security practices among Dams Sector stakeholders
- 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

Goal 3: Detect Intrusion and Implement Response Strategies

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

Goal 4: Sustain Security Improvements

- Widespread security awareness among sector, cross-sector, government, industry partners and 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

Goal 5: Secure-by-Design

- Development of partnership 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)

Goal 1: Measure and Assess Security Posture

- Implementation of training programs throughout the Dams Sector on the control system security recommended guidelines
- 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

Goal 2: Develop and Integrate Protective Measures

- Implementation of new protective tools and appropriate training
- Implementation of secure interfaces between ICS and business systems
- Identification, publication, and dissemination of best practices, including ones for securing connectivity with business networks and for providing physical and cybersecurity for remote facilities
- Development of high-performance, secure communications for legacy systems

Goal 3: Detect Intrusion and Implement Response Strategies

- Implementation of intrusion detection software in monitoring sector ICSs, publication of related best practices and guidelines and provision of related training
- Implementation of training programs for new intrusion detection software and any associated updates to response, identification and reporting procedures
- Development of control systems simulators to perform the operator training
- Development of training for control room operators in identifying and reporting unusual events, breaches, and anomalies from a cyber event
- Implement configuration management procedures and test beds for patch installations
- Development of public communication strategies and dissemination of public safety training literature on consequences of a disruption from a cyber event

Goal 4: Sustain Security Improvements

- 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 life cycle investment framework for cybersecurity that can be tailored to the Dams Sector and its members
- Formation of partnerships between government and industry and designation of roles to help sustain best practices in industry

Goal 5: Secure-by-Design

- 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)

Goal 1: Measure and Assess Security Posture

- Development of fully automated security state monitors in most Dams control systems networks
- Industry-wide active assessment of ICS security profiles including benchmarks against other sectors

Goal 2: Develop and Integrate Protective Measures

- Secure integration of ICS and business systems

Goal 3: Detect Intrusion and Implement Response Strategies

- Development and installation of self-healing control system architecture throughout Dams Sector
- Implementation of real-time intrusion detection and prevention systems

- Development of control systems security certification program for operators

Goal 4: Sustain Security Improvements

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

Goal 5: Secure-by-Design

- 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 technology 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

This roadmap is published under the auspices of the U.S. Department of Homeland Security (DHS). The need for the roadmap was identified by the Dams Sector Security Education Workgroup, which is composed of members from the Dams Sector Coordinating Council (SCC) and the Dams Sector Government Coordinating Council (GCC).

The SCC and the GCC were established as a partnership mechanism to collaborate with the DHS Dams Sector-Specific Agency in sector-wide security and protection activities focused on the Dams Sector. For more information, contact: dams@dhs.gov.

Homeland
Security