Roadmap to Secure Control Systems in the Water Sector

March 2008

Developed by

Water Sector Coordinating Council Cyber Security Working Group

Sponsored by

American Water Works Association

Homeland Security

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Roadmap to Secure Control Systems in the Water Sector	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Water Sector Coording Council Cyber Security Working Group,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**48**	

Members of the Water Sector Coordinating Council Cyber Security Working Group

The *Roadmap to Secure Control Systems in the Water Sector* was developed by the Water Sector Coordinating Council (WSCC) Cyber Security Working Group (CSWG) with support from the Department of Homeland Security National Cyber Security Division and American Water Works Association. Leadership for this project was provided by Seth Johnson, WSCC-CSWG Representative; Bruce Larson, WSCC-CSWG Representative; Dave Edwards, Process Control Systems Forum Water and Wastewater Representative; and Kevin Morley, WSCC Secretariat.

Acknowledgements

The Water Sector Coordinating Council (WSCC) Cyber Security Working Group (CSWG) would like to acknowledge everyone who contributed to the development and finalization of the *Roadmap to Secure Control Systems in the Water Sector*. In accordance with the National Infrastructure Protection Plan partnership model, the WSCC Cyber Security Working Group worked in close collaboration with the individuals identified below and devoted significant time, energy, effort, and resources to develop a *Roadmap to Secure Control Systems in the Water Sector*. This roadmap also meets the cyber-related criteria identified by the Government Accountability Office.[1] Sponsorship for roadmap activities came from the American Water Works Association (AWWA), which funded two roadmap development meetings, and the Department of Homeland Security, which funded the meeting facilitation.

WSCC Cyber Security Working Group (WSCC-CSWG)

Paul Bennett, New York City Department of Environmental Protection

Amy Beth, Denver Water

Cliff Bowen, California Department of Health Services

Jake Brodsky, Washington Suburban Sanitary Commission

Erica Brown, Association of Metropolitan Water Agencies

Kim Bui, San Antonio Water System

Vic Burchfield, Columbus Water Works

Richard Castillon, Orange County Sanitation District

Rick DaPrato, Massachusetts Water Resources Authority

Kim Dyches, Utah Department of Environmental Protection

Patrick Ellis, Broward County Water and Wastewater Services

Dave Edwards, Process Control Systems Forum/ Metropolitan Water District of Southern California

Rod Graupmann, Pima County Waste Water Management

Christina Grooby, Santa Clara Valley Water District

Darren Hollifield, JEA

Seth Johnson, Water Sector Coordinating Council Cyber Security Working Group Representative/formerly of Santa Clara Valley Water District

Bruce Larson, Water Sector Coordinating Council Cyber Security Working Group Representative/American Water

Carlon Latson, Denver Water

Tony McConnell, Washington Suburban Sanitary Commission

Kevin Morley, Water Sector Coordinating Council Secretariat/American Water Works Association

Jerry Obrist, Lincoln Water

Elissa Ouyang, California Water Service Company

Kevin Quiggle, Detroit Water and Sewage Department

Alan Roberson, American Water Works Association

Candace Sands, EMA Inc.

Cheryl Santor, Metropolitan Water District of Southern California

Birute Sonta, Metropolitan Water Reclamation District of Greater Chicago

Keith Smith, Metropolitan Water Reclamation District of Greater Chicago

Greg Spraul, Environmental Protection Agency Water Security Division

Walt Wadlow, Santa Clara Valley Water District

Stan Williams, Santa Clara Valley Water District

Ray Yep, Santa Clara Valley Water District

Facilitators:

Jack Eisenhauer and **Katie Jereza**, Energetics Incorporated

Table of Contents

Executive Summary

Today's industrial control systems (ICS) environments are incredibly complex assemblages of technology, processes, and people that work together to successfully carry out the missions and business functions of an organization. These systems have improved water and wastewater service and increased reliability in those infrastructures. As ICS have become more affordable and easier to use, most utilities have chosen to adopt them for process monitoring and/or control.[2] This reliance on ICS has left the water sector and other dependent critical infrastructures—such as energy, transportation, and food and agriculture—potentially vulnerable to targeted cyber attack or accidental cyber events.

> "Our information infrastructure—including... embedded processors and controllers in critical industries—increasingly is being targeted for exploitation and potentially for disruption or destruction."
>
> — *Annual Threat Assessment of the Intelligence Community (p. 15)*
> *J. Michael McConnell, Director of National Intelligence, February 7, 2008*

The Industrial Control Systems Security Imperative

Cyber threats to ICS are changing and growing.[2] Computer attackers are seeking new targets and criminal extortion is increasing. ICS security is no longer simply about blocking hackers or updating anti-virus software. A new underground digital economy now provides a multi-billion dollar incentive for potential adversaries to exploit ICS vulnerabilities.[3]

In today's highly dynamic and expanding digital economy, much of the ICS that operate our current water sector infrastructure are being used in ways that were never intended. Many ICS were designed decades ago with little or no consideration of cyber security. Increasing connectivity, the proliferation of access points, escalating system complexity, and wider use of common operating systems and platforms have all contributed to heightened security risks. Any interruption of a clean and safe water supply could erode public confidence or, worse, produce significant public health and economic consequences.

Industry Leadership

The urgent need to mitigate the risks associated with cyber systems has prompted industry and government leaders to step forward and collaborate on a unified security strategy. Their efforts have produced this *Roadmap to Secure Control Systems in the Water Sector,* which presents a vision and supporting framework of goals and milestones for reducing the risk of ICS over the next ten years. This strategic framework enables industry and government to align their programs and investments, improving ICS security quickly and efficiently. The roadmap integrates the insights and ideas of a broad cross-section of asset owners and operators, industrial control systems experts, and government leaders who met during workshops held in September and December 2007.

The Vision

By implementing this roadmap, water sector industry leaders believe that within 10 years, ICS throughout the water sector will be able to operate with no loss of critical function in vital applications during and after a cyber event. This vision confronts the formidable technical, business, operational, and societal challenges that lie ahead

Vision for Securing Industrial Control Systems in the Water Sector

In 10 years, industrial control systems for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event.

in strengthening the resilience of critical systems against increasingly sophisticated cyber attacks.

Organizations in the water sector have long recognized that it is neither practical nor feasible to fully reduce the risk of all assets from natural, accidental, or intentional damage. However, the water sector's track record of protecting public health and the environment reflects an effective approach to managing risk. This approach combines the proper level of risk mitigation measures with the most appropriate response and recovery to adequately achieve acceptable levels of security. Building on this approach, the industry's vision for securing water sector ICS focuses on critical functions of the most critical applications—those that, if lost, could result in human health impacts, loss of life, public endangerment, environmental damage, loss of public confidence, or severe economic damage.

A Strategic Framework

Roadmap Scope

This roadmap considers all variables for mitigating vulnerabilities and reducing the risk of industrial control systems in the water sector, including:

- Water and wastewater stakeholders and infrastructures
- Partnerships
- Critical functions and applications
- Near-, mid-, and long-term cyber security activities
- 10-year time frame

The water sector will pursue the following strategic goals in an effort to realize the vision of this roadmap. These goals are the essential building blocks of an effective risk management strategy.

Develop and Deploy ICS Security Programs. Cross-functional cyber security teams, including executives, information technology (IT) staff, ICS engineers and operators, ICS manufacturers, and security subject matter experts, will work collaboratively to remove barriers and create policies that will reduce security vulnerabilities and accelerate security advances.

2018 *Over the next 10 years, utilities throughout the water sector will have ICS security programs that reflect changes in technologies, operations, standards, regulations, and threat environments.*

Assess Risk. Community water and wastewater systems will have a thorough understanding of their current security posture, helping them to determine where ICS vulnerabilities exist and implement timely remediation.

2018 *Within 10 years, the water sector will have a robust portfolio of ICS recommended security practice analysis tools to effectively assess risk.*

Develop and Implement Risk Mitigation Measures. When vulnerabilities are identified, risk will be assessed and mitigation measures will be developed and applied to reduce risk, as appropriate.

2018 *Within 10 years, the water sector will have cost-effective security solutions for legacy systems, new architecture designs, and secured communication methods.*

Partnership and Outreach. Close collaboration among stakeholders and a strong and enduring commitment of resources will accelerate and sustain widespread adoption of ICS security practices over the long term.

2018 *Over the next 10 years, water asset owners and operators will be working collaboratively with government and sector stakeholders to accelerate security advances.*

The Challenges Ahead

Significant barriers exist to achieving the goals of the vision for securing ICS in the water sector. Because the requirements to mitigate vulnerabilities and reduce risk are not fully understood, many IT staff and ICS engineers and operators have difficulty collaborating on ICS security improvements. Few executives recognize the reality of ICS security threats

and their growing liabilities. Yet ICS risks are rapidly changing and growing. The business case for implementing ICS security has not been established. Thus, the available resources for and focus on ICS security improvements and solutions are limited. Managing change, such as installing security patches, is difficult in operating systems that have little room for error.

A paradigm shift in management priorities is necessary to achieve the goals outlined in this document. Many of today's risk mitigation products are burdensome and difficult to understand.[3] Coordination and information sharing between industry, government, and ICS manufacturers is also difficult, primarily because the specific roles and responsibilities in this emerging area are still being defined. Without due consideration of these and other challenges, a reliable, resilient water sector will not be possible in the future.

A Call to Action

The *Roadmap to Secure Control Systems in the Water Sector* will continue to evolve as industry reacts to cyber threat environments, business pressures, operational constraints, societal demands, and unanticipated events. While it does not cover all pathways to the future, this roadmap does focus on what its contributors believe to be a sound framework that addresses the most significant ICS challenges within the next 10 years. However, implementing the needed changes will involve the most difficult and complex steps toward achieving the desired results. To that end, the industry has outlined an industry-managed process to create, launch, and manage ICS security initiatives that are aligned with this roadmap.

Exhibit 1 Key Stakeholder Groups and Sample Members

Implementing this roadmap will require the collective commitment, collaboration, resources, and efforts of key stakeholders (Exhibit 1) throughout the ICS lifecycle. Strong leadership, action, and persistence is needed to ensure that important issues receive adequate support and resources. In addition, achieving early successes is important to maintaining momentum generated by the roadmap and convincing asset owners and stakeholders that the control systems security framework can work. While the precise roles of organizations in implementing this roadmap have not yet been determined, they will take shape as the roadmap is disseminated and reviewed by those engaged. The contributors of 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.

A Sustainable Approach

The risk management planning process must include constant exploration of emerging ICS security capabilities, vulnerabilities, consequences and threats.[4] Because the ICS security concepts described in this roadmap are intentionally broad based, the specific details of assessing risk and employing appropriate risk mitigation strategies will be developed in a technical plan. As the water sector pursues the strategies contained in the roadmap and technical plan, it will continue to review, assess, and adjust the mix of activities that will improve ICS security today and in the future.

I. Introduction

Leaders from the drinking water and wastewater industries (water sector) and the government have recognized the need to plan, coordinate, and focus ongoing efforts to improve industrial control systems (ICS) security. These leaders concur that an actionable path forward is required to address critical needs and gaps and to prepare the sector for a secure future. Their support helped to launch a public-private collaboration to develop this *Roadmap to Secure Control Systems in the Water Sector*. The roadmap focuses on the goals and strategic milestones for improving the security of ICS in the water and wastewater infrastructures over the next decade.

The roadmap content is the result of two meetings held by members of the Water Sector Coordinating Council (WSCC). The vision and strategic framework were designed by 30 experts during a workshop held on September 20, 2007, in San Jose, California. The WSCC Cyber Security Working Group (CSWG) developed more specific details of the roadmap, including milestones, challenges to achieving them, and potential solutions, during a meeting held on December 20, 2007, in Washington, D.C. The roadmap project was developed by the WSCC-CSWG and jointly sponsored by the American Water Works Association (AWWA) and the U.S. Department of Homeland Security National Cyber Security Division. For more information on the roadmap development process, please refer to Appendix A.

Roadmap Purpose

The roadmap builds on existing government and industry efforts to improve the security of ICS. It is the culmination of two years of collaboration among members of the water sector to examine problems and solutions for ICS security. The purposes of this roadmap are as follows:

- Define a consensus-based framework that articulates strategies of owners and operators in the water sector to manage and reduce the risk of ICS.
- Produce a broad-based plan for improving security preparedness, resilience, and response/recovery of ICS over the next 10 years.
- Guide efforts by industry, academia, and government to plan, develop, and implement ICS security solutions.
- Promote extensive collaboration among key stakeholders to accelerate ICS security advances throughout the water sector.

Roadmap Scope

The roadmap—combined with other initiatives—aims to provide a framework to address the full range of needs for mitigating cyber security risk of ICS across the water sector. For this roadmap, ICS are defined as the facilities, systems, equipment, services, and diagnostics that provide the functional control and/or monitoring capabilities necessary for the effective and reliable operation of the water sector infrastructure. While recognizing the importance of physical protection, this roadmap focuses on the cyber security of ICS. It does not specifically address the security of other business or cyber systems, except as they interface directly with the water sector ICS. This roadmap covers goals, milestones, and activities over the near (0-1 year), mid (1-3 years), and long term (3-10 years). Security activities encompass recommended practices, outreach, training, certifications, software patches, next-generation technologies, change management, information exchange, and implementation.

Roadmap Organization

The remainder of the roadmap is organized as follows:

- **Section II** describes the fundamental concepts associated with the current state of ICS security in the water sector including: (i) the missions and business functions ICS support; (ii) the major control components used in the water sector; (iii) the unique attributes of ICS systems and how they have changed over the

past decades to meet the sector needs; and (iv) an overview of ICS security risk, including vulnerabilities, consequences, and reported cyber events.

- **Section III** discusses the fundamental trends driving ICS security that the water sector must consider while preparing for the future, including: (i) business environments; (ii) cyber technologies; (iii) water operations; and (iv) societal needs.
- **Section IV** describes a coherent strategy for achieving the vision and goals of the water sector for securing ICS over the next 10 years, including: (i) develop and deploy ICS security programs; (ii) assess risk; (iii) develop and implement risk mitigation measures; and (iv) partnership and outreach.
- **Section V** describes a process for turning ideas into actions and proposes the main roadmap implementation steps, including: (i) socialize roadmap; (ii) roadmap oversight and project coordination; (iii) initiate and implement new roadmap activities; and (iv) sustain efforts.
- **Section VI** provides water sector contacts to find more information about this roadmap.

II. Industrial Control Systems Use in the Water Sector

A clean, safe, and reliable water supply—and the water system that delivers it—is at the heart of everyday life. Humans need water to survive. Businesses rely on water to operate and create products. Critical infrastructures, such as energy, transportation, and food and agriculture, depend on the water infrastructure for sustaining the flow of crucial goods and services. In addition, properly treated wastewater is vital for preventing disease and protecting the environment. Safeguarding the water sector against accidental impacts and purposeful attack is paramount. Any prolonged disruption of water supply could be devastating to the American people and the U.S. economy.

The water sector has a long and successful history of protecting public health and the environment. Many of the measures necessary to safeguard the water supply are in place to address unintentional contamination from natural disasters. Over the last few years, the water sector has also implemented additional measures to protect its infrastructure from deliberate attacks, such as physical assault, intentional contamination, and cyber intrusion.

Improving water service and sustainability, while maintaining affordability, has led to an increased dependence on IT. Nearly all efforts to enhance operations, reduce costs, and improve overall return on investments rely on an IT infrastructure, which supports a utility's vital assets and functions. While the use of IT systems within ICS architectures has created huge gains in reliability and productivity, they have also made the sector increasingly vulnerable to malicious cyber attack.

Supporting Missions and Business Functions

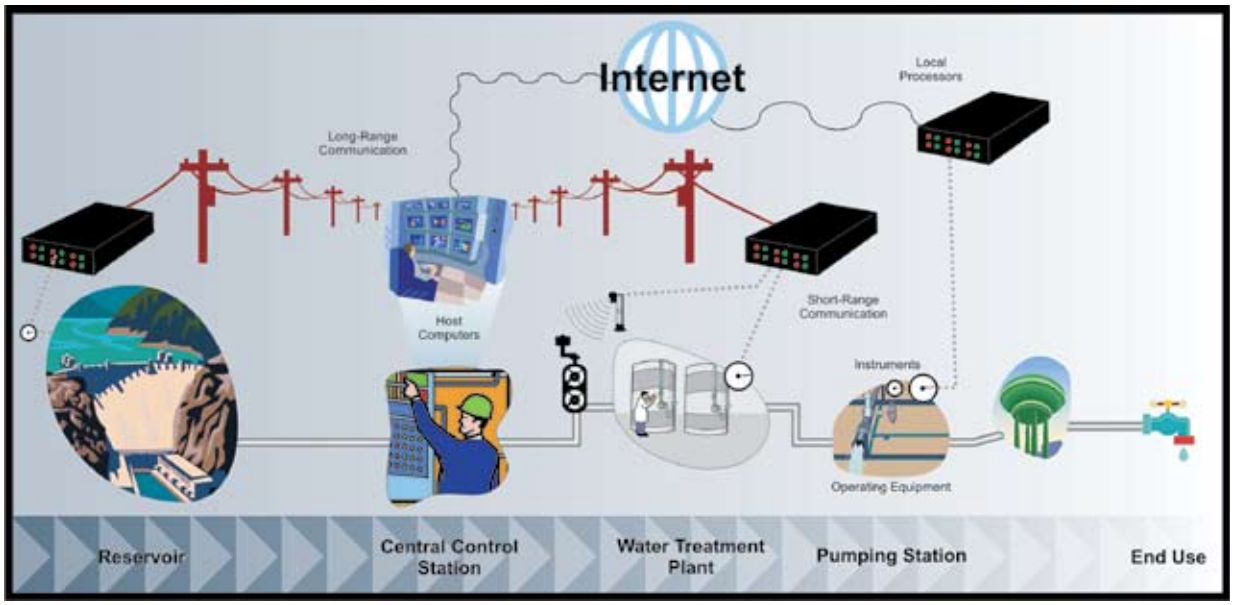
Water sector utilities depend on ICS to successfully carry out their missions and business functions. These systems allow for the monitoring of source water, continuous control of the treatment processes, and the high quality and delivery of finished water. The water sector uses ICS to help manage treatment and distribution operations and remotely monitor, and sometimes control, pressures and flows in water and wastewater pipelines. In addition, ICS perform data logging, alarming, and diagnostic functions so that large, complicated process systems can be operated in a safe manner and maintained by a centrally located and relatively small staff.

Industrial Control Systems (ICS) Monitor and/or Control a Water System

Industrial control systems are computer-based facilities, systems, and equipment used to remotely monitor and/or control critical process and physical functions. These systems collect data from the field, process and display this information, and then, in some systems, relay control commands to local or remote equipment.

ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC).[5] SCADA systems are highly distributed systems used to control geographically dispersed assets, where centralized data acquisition and control are critical to system operation. In the water sector, they are used in water distribution and wastewater collection systems. A DCS is a control architecture that supervises multiple, integrated sub-systems responsible for controlling the details of a localized process, such as water and wastewater treatment. PLCs are computer-based solid-state devices that control industrial equipment and processes. Because the differences in these control systems can be considered subtle for the scope of this document—which focuses on the integration of cyber security into these systems—SCADA

Exhibit 2.1 Components of Typical Industrial Control System in the Water Sector



Source: GAO (07-1036)

systems, DCS, and PLC systems will be referred to as ICS unless a specific reference is made to one (e.g., field device used in a SCADA system).

Major Control Components

ICS components comprise a central control station with one or more host computers, local processors, instruments, and operating equipment. Exhibit 2.1 depicts the major components of a typical ICS in a water treatment and distribution facility.[6] The components operate under a proliferation of control loops, human-machine interfaces (HMIs), and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures. The components communicate over short- and long-range channels, including the Internet and public-switched telephone networks using traditional cables or wireless media.

Central Control Station

The brain of any ICS is the central control station. It acts as the master unit, while local processors located at remote field sites usually act as slave units. Central control stations utilize one or more host computers to provide the graphical displays as well as the necessary computational and networking horsepower. They also use data historians to log all process information within an ICS. Input/output (I/O) servers are used to collect, buffer, and provide access to process information from the local processors. The sophistication of the central control station varies with the size and location of the water system. For example, a large metropolitan water and wastewater system may use modern process control systems to monitor and control their distribution network, the major treatment plants, and the wastewater collection systems. In small rural systems, a variety of basic and intermediate control systems technologies may be in place because the utility does not have the economic base of a large system, nor the personnel with the training to properly maintain advanced control systems.

Human Machine Interface

Operators interact with the system or process through the HMI. It allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. Control engineers use HMI to configure set points or control algorithms and parameters in the control system. The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. The location, platform, and interface may

vary a great deal. For example, an HMI could be a dedicated platform in the central control station, a laptop on a wireless local area network (LAN), or a browser on any system connected to the Internet.

Local Processors

Local processors, such as PLCs, remote terminal units (RTUs), and intelligent electronic devices (IEDs), allow for automatic control of process instruments and operating equipment. These devices acquire data, communicate to other devices, and perform local monitoring, processing, and control. Some applications require monitoring devices to be located at isolated equipment sites, pump stations and wells, or along a distant stretch of pipeline. The processors are equipped with input channels for sensing or metering; output channels for control, indication, or alarms; and a communications port, such as wireless radio interfaces.

Instruments and Operating Equipment

Water and wastewater systems consist of measurement points that need to be monitored for optimal process control. Such measurements are the basis for maintaining reliable storage, treatment, and distribution performance. Water sector instruments may provide online measurements of chlorine, dissolved oxygen, color/turbidity, conductivity, pH, pressure, fluid level, flow rate, and other critical elements. However, many tests continue to remain offline. In more sophisticated systems, sensors communicate with local processors to control valve, pump, and mixer operations. For example, maximum efficiency can be accomplished when pumps are instructed to operate at off-peak times. Some systems work in conjunction with modeling software to instruct the local processor to start or stop pumps in anticipation of changes in demand.

Evolution of ICS and Today's Risks

In the United States, there are approximately 160,000 public water systems serving about 250 million people and more than 16,000 wastewater utilities serving more than 225 million people. The Water Resources Foundation estimates that revenues in the U.S. water industry amount to more than $150 billion a year. Though ICS offered water utilities numerous benefits when they appeared on the market, few utilities could afford them; the systems required specific knowledge of software, hardware, and communications technology and had high capital costs. ICS have since become more affordable and easier to use, and today most water utilities use ICS for process monitoring and/or control.[2] According to a 2007 ARC Advisory Group study, the water sector spent $214 million on ICS systems in 2006.[7] That number is forecasted to reach more than $275 million in 2011.

In today's highly dynamic and expanding digital economy, much of the current water sector infrastructure and the ICS that operate it are being used in ways that were never intended. Many ICS were designed decades ago with little or no consideration for cyber security. Increasing connectivity, the proliferation of access points, escalating system complexity, and wider use of common operating systems and platforms have all contributed to heightened security risks.

Cyber Security Threats

Throughout history, water systems have played a prominent role in political actions and military operations. The vital role of water in daily life and economic activity underscores its importance to a secure and stable world. Consequently, any disruption or contamination caused by a cyber event would generate a great deal of publicity. Vast reservoirs and tens of thousands of miles of aqueducts and pipelines make the U.S. water sector a challenge to secure. The elevated interconnectivity, accessibility, and use of ICS further expose these critical assets. As a result, the water sector is vulnerable to potential cyber attack or natural disasters.

Evidence suggests that contamination of U.S. water supplies through cyber event failures could produce significant public health and economic consequences. Experience with naturally occurring contamination events has demonstrated that costs to the community may be considerable. For example, the 1993 Cryptosporidium outbreak in Milwaukee, Wisconsin, caused illness in more than

Water Sector Industrial Control Systems Risk Today

Some of the most serious constraints in design and changes in how ICS are currently used in the water sector include:

- **Design Limitations.** Historically, ICS have been designed for productivity and reliability; as a result, cyber security was not considered. In addition, limited computing resources have constrained the control system's ability to perform additional security functions. Although older legacy systems may operate in more independent modes, they tend to have inadequate password policies and security administration, no data protection mechanisms, and information links that are prone to snooping, interruption, and interception. These legacy ICS have very long service lives (about 20 years), and could remain vulnerable.
- **More Open Environments.** In the past, ICS systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and communications technology. Infiltrating these systems often required specific knowledge of individual system architectures and physical access to system components. To enhance interoperability, architectures and software packages became more standardized using commercial off-the-shelf technologies; this elevates system accessibility to potential cyber attack.
- **Increased Connectivity.** Today's operating needs have created a technology convergence of physical and cyber infrastructures. Automation has increased due to the need to improve operational efficiencies and workforce shortages. ICS are increasingly connected to a company's enterprise system, rely on common operating platforms, and are accessible through the Internet. While these changes improve water system operability, they have also created serious vulnerabilities because there has not been a concurrent improvement in security control systems features.
- **Increased Complexity.** The demand for real-time business information has increased system complexity: access to ICS is being granted to more users, business and control systems are interconnected, and the degree of interdependence 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 led to challenges in coordinating network security between these two groups.
- **System Accessibility.** Even limited use of the Internet exposes ICS to all of the inherent vulnerabilities of interconnected computer networks (e.g., viruses, worms, hackers, and terrorists). In addition, control channels use wireless or leased lines that pass through commercial telecommunications facilities, providing minimal protection against forgery of data or control messages. Legacy systems often allow "back-door" access via connections to third-party contractors and maintenance staff.
- **Supply Chain Limitations.** There are few manufacturers of software, hardware, and ICS for the water sector. A disruption in the ICS supply chain could interfere with a utility's response to a failure in the ICS.
- **Information Availability.** Manuals and training videos on ICS are publicly available, and many hacker tools can now be downloaded or purchased on the Internet and applied with limited system knowledge. Attackers do not have to be experts in ICS operations.

400,000 persons, and was estimated by the Center for Disease Control (CDC) to cost a total of $96 million, including over $31 million in lost wages and productivity.[8]

Maintaining consumer confidence is an ongoing challenge for the water industry, even without having experienced an attack. Despite the fact that U.S. water companies and utilities maintain some of the highest quality public drinking water in the world, a cyber attack on one portion of the water supply could erode public confidence in the safety of drinking water across the country. For example, a disaster preparedness drill conducted in California in 2000 almost caused widespread panic throughout the state.[9] After simulating the destruction of the Lake Nacimiento Dam, management had to quickly respond through mass media to counter the subsequent panic.

Water supplies do not actually have to be contaminated for disruption to occur. Hoaxes or threatened incidents of contamination can pose considerable management and response challenges for water utilities and political leaders. For example, when the village of Orwell, Ohio, received a threat against its water supply in November 2004, local leaders advised citizens not to use their tap water for consumption while the incident was being investigated.[10] Village employees directly contacted more than a thousand homes in the affected area via phone or by paper notice. The incident occurred over the Thanksgiving holiday and created huge demands on a small community despite being a hoax.

At the 2008 SANS SCADA Security Conference, U.S. Central Intelligence Agency senior analyst Tom Donahue announced that "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."[13]

How Can Cyber Events Affect Water Systems?

Cyber events can affect water system operations in a variety of ways, some with potentially significant adverse effects in public health. Cyber events could do the following:

- **Interfere with the operation of water treatment equipment, which can cause chemical over- or under-dosing**
- **Make unauthorized changes to programmed instruction in local processors to take control of water distribution or wastewater collection systems, resulting in disabled service, reduced pressure flows of water into fire hydrants, or overflow of untreated sewage into public waterways**
- **Modify the control systems software, producing unpredictable results**
- **Block data or send false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions**
- **Change alarm thresholds or disable them**
- **Prevent access to account information**
- **Although many facilities have manual backup procedures in place, failures of multiple systems may overtax staff resources—even if each failure is manageable in itself**
- **Be used as ransomware**

Real Cyber Events

Reported cyber attacks and unintentional incidents involving the water sector demonstrate the potential impact of a cyber event. The following incidents illustrate the consequences of real cyber events:

- Insider hacks into sewage treatment plant (Australia, 2001)—A former employee of the software developer repeatedly hacked (46 occasions) into the SCADA system that controlled a Queensland sewage treatment plant, releasing about 264,000 gallons of raw sewage into nearby rivers and parks.[6]
- Equipment malfunction at water storage dam (St. Louis, MO, 2005)—The gauges at the Sauk Water Storage Dam read differently than the gauges at the dam's remote monitoring station, causing a catastrophic failure which released one billion gallons of water.[6]
- Intruder plants malicious software in a water treatment system (Harrisburg, PA, 2006)—A foreign hacker penetrated security of a water filtering plant through the internet. The intruder planted malicious software that was capable of affecting the plant's water treatment operations.[6]
- Reported Vulnerability (Aurora 2007)—CNN reported a control system vulnerability that could damage generators and motors. [11]
- Intruder sabotages a water canal SCADA system (Willows, CA, 2007)—An intruder installed unauthorized software and damaged the computer used to divert water from the Sacramento River. [12]
- CIA Confirms Cyber Attack Caused Multi-City Power Outage (New Orleans, 2008)—CIA has information that cyber intrusions into utilities (followed by extortion demands) have been used to disrupt power equipment in several regions outside the United States.[13]

III. Future Trends and Drivers Influencing Industrial Control Systems Security

The dynamic cyber environment challenges the ability of water utilities to combat new threats. As business environments, cyber technologies, water operations, and societal needs continue to reshape the cyber security landscape, the security posture of the water sector will be increasingly challenged (see Exhibit 3.1). Without consideration of future trends and drivers, the water sector could be unprepared for the formidable challenges ahead.

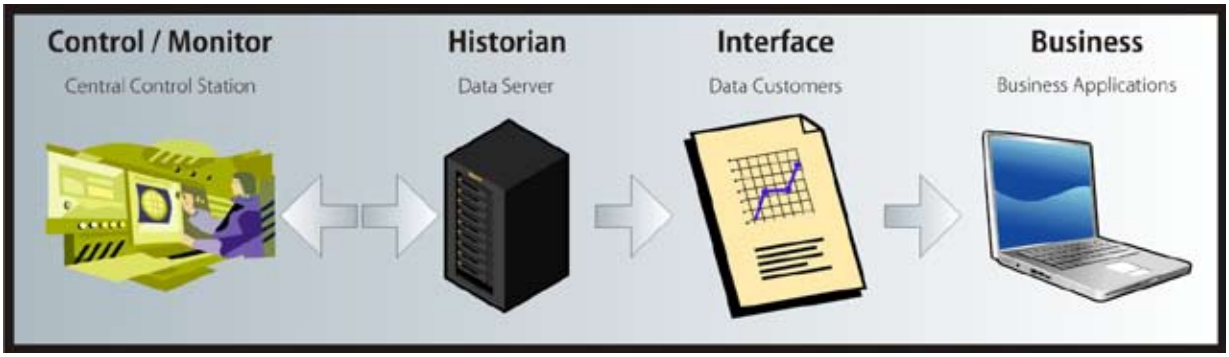
Business Environments

Several dynamics within a water system's community place significant strategy demands on utility executives who must work effectively in these contexts. For example, the cultural resistance to change is difficult to overcome. Aligning the short-term horizon of elected officials with the long-term nature of utility management decisions can be a daunting task. Turnover of elected and other community leaders requires constant re-education efforts. Water sector utilities are a "hidden infrastructure," which causes residents to undervalue the service provided. Seasonal weather patterns (e.g., summer and winter) and climatic extremes (e.g., floods and droughts) create uncertainties in water demand patterns, making both short- and long-term investment strategies complex and difficult. As such, the water sector may continue to struggle with generating and sustaining support of a governing body, private industry, and the general community for cyber security.

Exhibit 3.1 Future Trends and Drivers Influencing Industrial Control Systems (ICS) Security

Business Environment	• Ability to change is slow due to fiscal constraints • Changing weather patterns create cyclic demand on water production • Increasing need for real-time business information • Increasing convergence of information and operations technologies • Aging workforce, staff turnover, and reduction in experienced personnel
Cyber Technologies	• Changing and growing ICS threats and accidents • Accelerating pace of change in threat sophistication and the resulting impact of attack from these adversaries • Increasing use of electronic and wireless communications • Increasing use of open, non-proprietary systems
Water Operations	• Increasing need for faster operational response • Growing control and monitoring needs • Increasingly stringent water regulations increase instrumentation and monitoring requirements • Competing capital investments, such as upgrading an aging infrastructure
Societal Needs	• Maintaining public confidence in water quality • Growing population and expanding water scarcity

Exhibit 3.2 Integration of Industrial Control Systems with Business Systems



The increasing need for real-time business information, driven by the need to reduce costs, increase water distribution efficiencies, and comply with operational and financial regulations, will require a new approach to IT management, such as system consolidation and integration (Exhibit 3.2). For example, ICS will increasingly operate with data and business systems to support emerging management functions. Efforts to seamlessly integrate these systems will also shape ICS security practices. In addition, the aging workforce is rapidly reaching retirement. Many key positions are not expected to be filled.[2] To do more with less staff, utilities are installing additional control systems to operate the assets, take readings, and record condition-monitoring data. Training programs will need to increase to educate operators on these newly installed technologies, and they must occur more regularly to address turnover in experienced staff.

Cyber Technologies

The threat environment is changing and growing.[2] A 2003 American Water Works Association Research Foundation (AwwaRF) report found more than 100 cases of actual, threatened, and disrupted plots to contaminate water supplies. Of those cases, 20 incidents involved actual contamination events, more than half of which occurred in modern water supplies with pressurized pipe distribution.[14] While few of these threats are attributed to cyber attackers, most executives, government officials, and vendors do not fully appreciate the potential threat that exists to the water infrastructure due to the risks created by vulnerabilities in control systems technologies.

Computer attackers are constantly looking for new targets, and criminal extortion schemes have already occurred.[15] In December 2006, an automated control systems vulnerability scanner was released, allowing individuals outside the utility with relatively little experience in control systems to quickly identify vulnerabilities. In a recent computer industry paper, experts agreed that attackers are forming a hacking industry, an underground economy that exploits control systems vulnerabilities for economic gain. Raimund Genes, chief technical officer of Trend Micro, estimates this underground digital economy generated more revenue than the $26 billion that legitimate security vendors generated in 2005.[16] The need for cyber security is real and is no longer about blocking hackers or updating anti-virus software to ensure that systems are functioning properly. Cyber threats are becoming more sophisticated and as new threats are introduced, the water sector must rapidly evolve.

Central control stations are increasingly communicating with remote process controllers via the Internet and wireless networks. Further integration of shared telecommunications technologies into normal business operations has spawned increased levels of interconnectivity among corporate networks, control systems, and the outside world. Continued expansion of the U.S. water sector has created still greater reliance on public telecommunications networks to monitor and communicate with those growing assets. To achieve higher levels of interoperability among various IT technologies, the water sector is shifting toward more open, non-proprietary systems. Increasing interconnectivity and openness exposes network assets to potential cyber infiltration and subsequent manipulation of sensitive operations in the water sector.

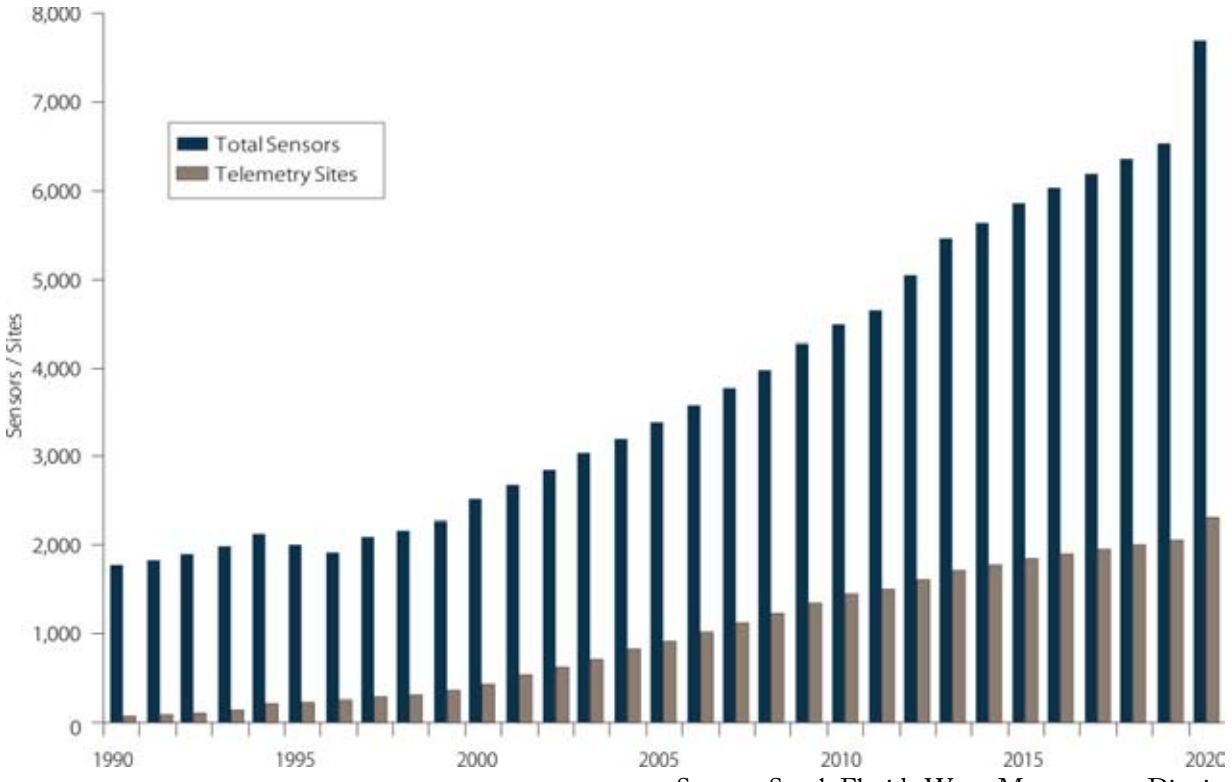
Water Operations

To minimize public exposure to contaminants or service disruptions, while providing additional time to evaluate the nature and severity of an abnormal event, operational response time requirements are increasing. New online contaminant monitoring systems will target an average up-time of at least 99.9 percent, or a mean time offline of no more than 10 minutes.[17] Population growth, combined with an increasing number of regulated contaminants, will greatly expand and complicate water systems. This complexity will lead to an exponential increase in the number of sensors and telemetry sites that will be needed to support additional monitoring and control throughout the system. Exhibit 3.3 illustrates the future sensor needs of a large community water system, the South Florida Water Management District, which currently operates and maintains approximately 1,800 miles of canals and levees, 25 major pumping stations, and about 200 large and 2,000 small water control structures.[18] For the next 10 years and beyond, the water sector must make a substantial reinvestment in infrastructure to replace worn-out drinking water pipes and associated structures (valves, fittings, etc.). The AWWA projects expenditures of $250 billion over 30 years may be required nationwide. Competing capital investments will aggravate already overstretched resources in the water sector and potentially limit the implementation of ICS security solutions.

Societal Needs

The public today wants a water utility, whether public or private, to be aware and responsive to their concerns. In the future, successful water utilities must also anticipate those concerns and be prepared with accurate facts and information. These issues are increasing customer service programs, including community outreach, educational programs, and establishment of innovative rate structures. In addition, population growth combined with source water limitations are elevating public awareness of the need to conserve, reuse, and recycle water. This heightened awareness is increasing the need for utilities to implement and promote both internal and external water efficiency programs, which further increases the use and complexity of ICS.

Exhibit 3.3 Example of a Large Water System's Future Sensor Needs



Source: South Florida Water Management District

IV. A Framework for Securing ICS in the Water Sector

Security measures that ensure the availability of safe drinking water, wastewater treatment, and the delivery of vital services, such as fire fighting, continue to be a top priority for the water sector. While much security work has focused on physical security—fences, guards, intrusion detection, etc.—efforts pertaining to the resiliency of industrial control systems (ICS) have become more urgent. Advances in securing ICS must go far beyond the pressing security concerns of today by taking a comprehensive approach that prepares for the needs of tomorrow.

Water sector utilities will need to understand and manage ICS risks, secure their legacy systems, conduct vulnerability assessments, apply security tools and practices, and consider next-generation systems—all within a publicly transparent and competitive business environment. Government has a large stake in the process because nearly all critical infrastructures depend on a reliable, safe, and clean water supply. Any sustained disruption could endanger public health and safety. However, ICS security must compete with other investment priorities, such as infrastructure repairs, upgrades, and expansion. A coordinated strategy that links and integrates the efforts of industry and government is needed to achieve mission-critical goals. This concept manifests itself in the water sector's vision statement and goals.

Vision

Based on sound risk management principles, the water sector has developed the following unified vision for ICS security:

In 10 years, industrial control systems for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event.

The vision emphasizes critical applications, because it is neither practical nor feasible to protect all of the water sector assets from cyber events. Many of these assets are not threat targets, some are not vulnerable, and some would not create serious consequences if disabled. Water systems in the U.S. vary according to size, source, treatment, and geography. These systems are tremendously diverse, ranging from very small, privately owned systems (such as mobile home parks) to huge, publicly owned systems serving millions of people. Reservoirs may contain a few million to several hundred billion gallons of water, making it logistically difficult to contaminate them with sufficient quantities of toxins to cause widespread illness. Across the U.S., there are almost three million miles of distribution pipes and collection lines. While there is concern about the vulnerability of distribution systems, these networks were designed to withstand some loss of capability without loss of critical function. In

Vision Terms Defined

Critical Applications: ICS for critical applications include components and systems that are indispensable to the safe and reliable operation of the water system. Criticality of an application is determined by the severity of consequences resulting from its failure or compromise. Such components may include controls for operating pumps or managing pipeline pressure.

Cyber Event: A cyber event occurs when a terrorist attack, other intentional act, natural disaster, or other hazard destroys, incapacitates, or exploits all or part of a control system network with the potential to cause economic damage, casualties, public harm, or loss of public confidence.

Loss of Critical Function: A critical function of a water system is any operation, task, or service that, were it to fail or be compromised, would produce major safety, health, operation, or economic consequences.

addition, water treatment can reduce the risk of conventional microbial contamination. By focusing on ICS systems for critical applications to prevent loss of crucial functions, the water sector can develop strategic goals and milestones that effectively protect the public, customers, assets, and shareholders.

ICS Security Goals

Realization of the vision requires concerted and focused efforts. The water sector has developed and will pursue a set of strategic goals articulating these ambitions. These goals will help focus security activities to accelerate progress in achieving the vision. As shown in Exhibit 4.1 and described below, a framework emphasizing a desired end state and aggressive set of milestones will provide a sound foundation for future cyber security initiatives.

- **Develop and Deploy ICS Security Programs.** Executives will recognize that ICS security is critical to fulfilling mission-critical goals. Cross-functional ICS security teams, including executives, IT staff, ICS engineers and operators, ICS manufacturers, and security subject matter experts, will work collaboratively to remove barriers and create policies that will reduce security vulnerabilities and accelerate security advances. Over the next 10 years, utilities throughout the water sector will have ICS security programs that reflect changes in technologies, operations, standards, regulations, and threat environments.
- **Assess Risk.** Community water and wastewater systems will have a thorough understanding of their current security posture to determine where ICS vulnerabilities exist and implement timely remediation. Vulnerability assessments will be integrated into cyber security plans. Security improvement performance will be measurable and consistent. By 2018, the sector will have a robust portfolio of ICS recommended security practice analysis tools to effectively assess risk.
- **Develop and Implement Risk Mitigation Measures.** When vulnerabilities are identified, protective measures will be developed and applied, as appropriate. Risk can be further reduced by adding multiple layers of security and redundant components. Control systems will be capable of self-diagnosis and real-time monitoring and alerting, while being easy to maintain and update. Within 10 years, the sector will have cost-effective security solutions for legacy systems, new architecture designs, and secured communication methods.
- **Partnership and Outreach.** Close collaboration among stakeholders and a strong and enduring commitment of resources will accelerate and sustain widespread adoption of ICS security practices over the long term. Federal stakeholders will maintain ICS threat support. Information sharing will be adequate and timely within the water sector, among critical infrastructures, and between government agencies. Over the next 10 years, water asset owners and operators will be working collaboratively with government and sector stakeholders to accelerate security advances.

These goals provide a logical framework for organizing the collective efforts of industry, government, and other key stakeholders to achieve the vision. To be successful, however, specific milestones must be accomplished in the 2008-2018 period. Projects, activities, and initiatives that result from the roadmap should be tied to the milestones shown in Exhibit 4.1.

Strategies for Securing ICS

Strategies for accomplishing the four goals presented in Exhibit 4.1 are summarized in Exhibits 4.2 through 4.7. Each goal presents distinct obstacles that must be overcome, requires specific achievements on an established timetable, and recommends potential solutions. The rapid pace of change in cyber technologies combined with uncertainties in markets, regulations, and risk require that the water sector stay vigilant and responsive to a variety of plausible futures. As the water sector pursues the strategies contained in this roadmap, it must review, assess, and adjust the mix of activities that will lead to success today and in the future.

Exhibit 4.1 Strategy for Securing Industrial Control Systems (ICS) in the Water Sector

Vision

In 10 years, industrial control systems for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event.

Challenges

- Limited collaboration between IT & ICS departments
- Limited executive recognition of ICS security threats & liabilities
- Business case for ICS security is not established
- No clear up-front security requirements
- Limited understanding of ICS risk factors
- Rapid pace of change in threat actors & vulnerabilities
- No ICS security training resources
- Limited resources to mitigate risk
- Difficult or impossible to integrate new technologies into legacy systems
- Managing change in mission critical systems
- Differing view points of sector partnerships
- Competing priorities limit resources
- Difficult to fully implement cyber-security across entire water sector

Goals

Develop and Deploy ICS Security Programs	Assess Risk	Develop and Implement Risk Mitigation Measures	Partnership and Outreach

Milestones

Near-Term (0-1 years)

- 80% of water sector executives recognize ICS security is mission critical
- IT staff and ICS engineers and operators coordinate ICS security efforts
- Integrate security as a key goal in every project plan
- Develop a recommended practices ICS security template for widespread use in the water sector
- Integrate & elevate ICS security requirements with vendor contracts
- Isolate ICS from public switched networks
- Integrate roadmap with Water Sector Specific Plan
- Develop ICS risk assessment & reporting guidelines published & available throughout the water sector
- Identify common metrics for benchmarking ICS risk (threat-vulnerabilities-consequence) in the water sector
- Develop ICS risk assessment tools, such as end-to-end, threat-vulnerabilities-consequence analysis capability for the water sector
- Establish working group for developing/maintaining recommended practices for ICS network architecture(s) for the water sector
- Develop cyber response protocol template
- ICS vendors start to implement or increase their cyber security features by 50%
- Identify and implement existing security features built into the devices
- Replace default security passcodes
- Develop effective federal & state incentives to accelerate investment to secure ICS technologies & practices
- Increase ICS security awareness between water sector, cross-sector, vendor & commercial partners
- Develop essential body of ICS security knowledge for information sharing

Mid-Term (1-3 years)

- Conduct sector-wide training on recommended practices ICS security template
- Integrate ICS security awareness, education, & outreach programs into water sector operations
- Conduct sector-wide training on risk assessment tools
- Reduce installation time of ICS patching
  - Frameware by 50%
  - Applications by 99.9%
- System design accommodates restarts
- Develop operator ICS security training program
- Adopt recommended practices for ICS security in the water sector
- Develop public communication channels to increase confidence in efforts to prevent or minimize impacts from a cyber event

Long-Term (3-10 years)

- Sustain roadmap activities in accordance with the Water Sector Specific Plan
- Water sector actively measures ICS security performance & benchmarks with other sectors
- Develop & implement self-defending ICS & infrastructure
- Require ICS security in operator certification
- Real-time security state monitoring for intrusions are commercially available
- Establish life cycle investment & framework for cyber security
- Government maintains ICS threat support
- Identify, understand, & disseminate timely ICS risk information within the sector & among its partners

End State

The water sector will have ICS security programs that reflect changes in technologies, operations, standards, regulations, and threat environments	The water sector will have a robust portfolio of ICS recommended security practice analysis tools to effectively assess risk	Security solutions for legacy systems, new architecture designs, and secured communication methods will be cost effective	Water asset owners and operators will work collaboratively with government and sector stakeholders to accelerate security advances

Goal: Develop and Deploy ICS Security Programs

Water sector organizations operate in a highly complex and interconnected world using IT systems and ICS. Organizations depend on both of these systems to accomplish their missions and to carry out their business functions and industrial operations. Explicit management decisions are necessary in order to balance the benefits gained from the use of IT and ICS systems with the overall risk. Managing risk is not an exact science. To secure IT and ICS systems, risk management must bring together the best collective judgments of the individuals responsible for the strategic planning and day-to-day operations of the entire organization.

Managing organizational risk related to IT and ICS systems begins with a fundamental commitment by senior leadership in the organization to make IT and ICS security a first-order mission/business requirement. This commitment ensures that sufficient resources are available in the design, development, implementation, operation, and disposition of IT and ICS systems to provide adequate levels of security, while meeting critical function expectations. IT and ICS security must be considered a strategic capability and an enabler of missions and business functions across the organization. Cross-functional ICS security teams, including executives, IT staff, ICS engineers and operators, and security subject matter experts, must work collaboratively to remove barriers and create policies that will reduce security vulnerabilities and accelerate security advances. To adequately reflect rapid changes in technologies, operations, standards, regulations, and threat environments, the utilities throughout the water sector must have ICS security programs that are reviewed and updated regularly.

An overview of the challenges, milestones, and potential solutions for developing and deploying ICS security programs in the water sector is shown in Exhibit 4.2.

Challenges

The complexity, diversity, and multitude of mission, business, and operation functions within an organization require an organization-wide approach to managing risk. However, obtaining an organization-wide perspective by all authorizing officials and senior leaders is a complex task. Strong commitment, direct involvement, and ongoing support do not exist from senior leaders because they are unaware of the magnitude of ICS security risk. The lack of an established business case for implementing ICS security has also kept executives from developing security policies that integrate IT with ICS security, and from institutionalizing these policies into the overall management structure.

There is a long-standing IT paradigm of one application running one server, owned by one plant or division. Silos—internal divisions such as plants, IT, distribution systems, and operations—exist because each of those disciplines has become very complex. Each silo has different objectives, needs, and levels of expertise, which can hinder collaboration—especially between IT and ICS, which have different security requirements, such as down time (i.e., periodic versus zero).

Legacy systems often have constrained resources and lack security functions. ICS components may not have the computing resources needed to retrofit these systems with current security capabilities. In addition, one single security product or technology cannot adequately protect an ICS. Doing so requires a combination of properly configured security controls and effective security policies. An effective cyber security strategy for an ICS should apply defense-in-depth, but this strategy is not well coordinated between vendors and users in the water sector system. Also, the water sector represents a small minority of the ICS market, which provides little incentive for vendors to pursue security activities specific to the water sector.

Defense-In-Depth

Defense-in-depth is a technique of layering security mechanisms so that the impact of a mechanism failure is minimized.

Potential Solutions

Effectively integrating security into an ICS will require the development and implementation of activities such as educating executives, defining and executing cyber security practices, and ongoing assessment for improvement. The industry must first identify recommended practices, such as connecting ICS and business networks. Recommended practices can provide insight on "quick fix" solutions—low-cost, high-value practices that can significantly reduce risk in the short term—and on long-term solutions to sustain security improvements. One "quick fix" for managing complexity has already been identified as a near-term milestone: the isolation of ICS from public-switched networks, including cable modems, direct dial modems, open T1s, and Internet access. This will significantly decrease opportunities for exploitation and improve the security posture of the infrastructure.

Security awareness is critical to obtaining buy-in from executives, IT personnel, and the vendor community. The industry needs an ICS security marketing strategy that includes socializing and collaborating with executives, IT, and operations. The state of California offers a model outreach program, which can be replicated in regions across the U.S. (Refer to Section VI for contact information.) To establish a business case for ICS security throughout the water sector, the industry must develop a white paper that analyzes the incentives and benefits of implementing ICS security. In addition, the Process Control Systems Forum is a venue for developing partnerships with vendors.

Successfully managing risk may necessitate reengineering the processes used to accomplish missions and execute business functions. By purposefully integrating IT and ICS security into the execution of missions and business functions, system operators can significantly reduce risk without adversely affecting operation.

Performance metrics are needed to help ensure that ongoing ICS security efforts are conducted consistently across the organization, as well as the entire sector. By establishing performance metrics, organizations can determine the degree to which security integration is occurring and measure progress. Automated collection of ICS security information, including incident reports and visualization tools for correlation purposes, will help accelerate ICS security efforts nationwide. To sustain these efforts, the sector should evaluate the needs to integrate this roadmap into the Water Sector Specific Plan.

Exhibit 4.2 Strategies for Developing and Deploying Industrial Control Systems (ICS) Security Programs

Goal — Develop and Deploy ICS Security Programs

Challenges

- Lack of resources within the water sector and time to establish ICS security specifications
- Limited executive recognition of ICS security threats and liabilities
  - Security is not included in overall risk management
  - Risk management typically limited to asset management
- Lack of awareness about ICS security risks
- Business case for ICS security has not been established throughout the water sector
- Lack of overall security policies that integrate ICS
- Individual plants operate in silos
- Lack of collaboration between IT staff and ICS engineers and operations
- Lack of coordination between vendors and users on a layered security model
- Difficult or impossible to integrate new technologies into legacy systems
- Water sector has minority of ICS market, which limits vendor response
- Implementation of security measures is often time consuming

Milestones

2008

Near-Term (2008-2009)

- 80% of water sector executives recognize that ICS security is critical to fulfilling their mission
- IT staff and ICS engineers and operators coordinate the development and implementation of ICS security efforts
- Integrate ICS security as a key goal in every project plan
- Develop a recommended practices ICS security template for widespread use in the water sector
- Integrate and elevate ICS security requirements with vendor contracts
- Isolate ICS from public-switched networks, including cable modems, direct-dial modems, open T1s, and internet access
- Integrate Roadmap to Secure Control Systems in the Water Sector with Water Sector Specific Plan

Mid-Term (2009-2011)

- Conduct sector-wide training on recommended practices ICS security template
- Integrate ICS security awareness, education, and outreach programs into water sector operations

Long-Term (2011-2018)

- Sustain roadmap activities in accordance with the Water Sector Specific Plan

End State (2018)

- The water sector will have ICS security programs that reflect changes in technologies, operations, standards, regulations, and threat environments

2018

Potential Solutions

- Identify recommended practices for connecting ICS and business networks
- Develop ICS security marketing strategy for water sector
  - Socialize and collaborate with executives throughout the water sector
  - Socialize and collaborate with IT and operations personnel throughout the water sector
  - Develop a white paper on the business case for ICS security, include an analysis of incentives and benefits of implanting cyber security
  - Create appropriate incentives to encourage investment in ICS security
  - Partner with Process Control Systems Forum to work with vendors
- Integrate IT and ICS security into risk and asset management frameworks
- Establish performance metrics
  - Enable automated collection of ICS security information, including incident reports and visualization tools for correlation

Goal: Assess Risk

Risk analysis is the process through which the three components of risk—threat, vulnerability, and consequence—will be collectively analyzed to determine the water sector's cyber security posture. For 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. 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 ICS assets enables water sector stakeholders to prioritize security needs and focus limited resources on the most urgent security issues. Risk assessment data are also necessary to build a sound business case for investment in creating, procuring, and implementing ICS security measures. Conducting these assessments for community water and wastewater systems requires a robust portfolio of ICS security recommended practice analysis tools.

An overview of the challenges, milestones, and potential solutions for assessing cyber risk in the water sector is shown in Exhibit 4.3.

Challenges

Assessing ICS risk remains difficult due to a lack of sufficient analysis and measurement tools. Threats, when known, are often hard to demonstrate and quantify in terms that are meaningful for decision makers. New vulnerabilities can be introduced when business or infrastructure networks increase connections with ICS networks, and when new technologies are integrated into the ICS. The highly dynamic threat environment, combined with the rapid pace of change in cyber technology, creates a significant dilemma. In an industry familiar with inertia, rapid identification of new vulnerabilities will be challenging.

A cyber event in the water sector can produce a complex web of consequences that spans many sectors of the economy and reaches well beyond the individual or community experiencing the event. The consequences of a loss of public confidence in a utility are often overlooked; however, it is a real target for adversaries that could be accomplished through an ICS incident. Together, these factors present real challenges to a manager's ability to define the magnitude of harm resulting from a cyber event.

Inadequate assessment capabilities limit the ability of companies to accurately define ICS security requirements. As a result, clear and up-front requirements do not exist. Because some executives do not understand what is required, resources to initiate risk assessment activities are not made available, leaving the development and implementation of risk assessments at a stand still.

Potential Solutions

Near-term activities include developing a risk matrix that reflects consensus on how to frame and define critical vulnerabilities and match them with appropriate mitigation strategies. Risk assessment tools—such as end-to-end, threat-vulnerability-consequence analysis and evaluation of cyber attack and response simulators—should be developed. Creating ICS risk assessment and reporting guidelines, as well as common metrics for benchmarking ICS risks, is essential to facilitating cost-effective and consistent assessments across the water sector. Although self-assessment tools are currently available, there are uncertainties about their use. Enhancing the risk assessment methodologies, frameworks for prioritizing control measures, and cost justification tools will greatly enhance the water sector's confidence in the accuracy and usefulness of these tools.

Adoption of industry-approved incident reporting guidelines and recommended practices will increase data on all aspects of risk and enable the development of more accurate analysis and modeling tools for assessing it. In addition, sharing lessons learned means that a company is more likely to have the knowledge required to respond quickly to ICS emergencies, even when appropriate security measures are not available. Sector-wide training on these tools will further enhance risk analysis capabilities across the sector.

Exhibit 4.3 Strategies for Assessing Industrial Control Systems (ICS) Risk

Goal — Assess Risk

Challenges

- Limited knowledge, understanding, and appreciation of ICS risk factors inhibit action
- Rapid pace of change in threat actors and vulnerabilities
- No clear, up-front ICS security requirements
- No resources to train and implement ICS security assessments

Milestones

2008

Near-Term (2008-2009)

- Develop ICS risk assessment and reporting guidelines, published and available throughout the water sector
- Identify common metrics for benchmarking ICS risk (threat-vulnerabilities-consequence) in the water sector
- Develop ICS risk assessment tools, such as end-to-end, threat-vulnerabilities-consequence analysis capability for the water sector

Mid-Term (2009-2011)

- Conduct sector-wide training on risk assessment tools

Long-Term (2011-2018)

- The water sector actively measures ICS security performance and benchmarks with other sectors

End State (2018)

- The water sector will have a robust portfolio of recommended ICS security practice analysis tools to effectively assess risk

2018

Potential Solutions

- Create an ICS risk matrix that balances threat, vulnerability, and consequence
- Set up and evaluate ICS attack and response simulators
- Enhance tools for owners and operators to conduct self-assessments
  - Risk assessment methodologies, frameworks for prioritizing control measures, and cost justification tools
- Increase adoption of industry-approved incident reporting guidelines and recommended practices
- Establish performance metrics
- Increase awareness of DHS/local security assessments
- Increase awareness of available federal, state, and local government ICS training.

In the long-term, establishing performance metrics to benchmark within and across other sectors will be essential to building an assurance case for cyber security programs.

Goal: Develop and Implement Risk Mitigation Measures

It is impractical—if not impossible—to ensure that an ICS is 100 percent secure at any point in time. Therefore, organizations seek to manage risk in order to achieve acceptable levels of security. Managing risk from ICS systems to operations, assets, individuals, other sectors, or the nation requires a holistic approach, such as the Risk Management Framework (Exhibit 4.4.).[4]

The framework represents a cyber security life cycle that facilitates continuous monitoring and continuous improvement in the security state of the ICS systems as well as the overall resiliency of the water sector organization. This approach can provide the utility with enough flexibility to quickly apply the proper level of risk mitigation measures to the most appropriate ICS systems to adequately protect the critical missions and business functions of the water sector organization.

As ICS vulnerabilities are identified, known risk mitigation measures can be applied and new solutions developed to meet emerging needs. For legacy systems, these measures often include applying proven recommended practices and

Exhibit 4.4 Example of an Industrial Control Sytems Risk Management Framework

security tools, implementing procedures and patches for fixing known security flaws, creating training programs for staff at all levels, and retrofitting security technologies that do not degrade system performance. Communication between remote devices and control centers, and between IT systems and ICS, requires secure links, device-to-device authentication, and effective protocols. However, the most comprehensive security improvements are realized with the development and adoption of next-generation ICS architectures, which are inherently secure and offer enhanced functionality and performance. These systems can provide defense-in-depth with built-in, end-to-end security.

Affordability of drinking water is one of the major missions of a utility. With significant investment hurdles facing the water sector, risk mitigation measures will be difficult to fully implement at current cost levels. As such, security solutions for legacy and new architecture designs and communication methods must be cost-effective within the next 10 years.

An overview of the challenges, milestones, and potential solutions for developing and implementing risk mitigation measures in the water sector is shown in Exhibit 4.5.

Challenges

Effectively managing risk requires significant resources and efforts from multiple organizations within the utility. For example, close coordination and collaboration among knowledgeable individuals (e.g., system architects, systems/security engineers, system administrators, physical security experts, personnel specialists, etc.) will ensure that the appropriate personnel, processes, hardware, software, firmware, or environmental components provide their designated security functionality (e.g., access control, identification and authentication, evaluating and accountability, system and communications protection, physical security, personnel security, incident response, contingency planning, etc.). However, limited resources make this process difficult to manage and can hinder progress.

Legacy systems are especially vulnerable to computing resource availability and timing disruptions. Many systems do not have desired features including encryption capabilities, error logging, and password protection. Integrating new technologies into these systems is especially difficult, or even impossible. For example, older versions of operating systems may no longer be supported by the vendor, making some patches useless. Typical next-generation ICS components have a lifetime of five years or more. For ICS, where technology has been developed for very specific use, the lifetime of the deployed technology is often 15-20 years longer.

Change management is paramount to maintaining both IT and ICS systems, yet significant gaps in the process remain. Unpatched systems represent one of the greatest vulnerabilities. Software

Exhibit 4.5 Strategies for Developing and Implementing Risk Mitigation Measures

Goal — Develop and Implement Risk Mitigation Measures

Challenges

- Limited resources to implement risk mitigation measures
- Difficult or impossible to integrate new technologies into legacy systems
  - Current ICS do not include effective security measures
  - Development pipeline is five years or more
- Managing change in mission critical systems
- No room for error when upgrading/patching ICS
- Action ability—how to develop risk mitigation products that owners and operators can understand and use
- Implementation and maintenance of password protected devices is burdensome

Milestones

2008

Near-Term (2008-2009)

- Establish working group for developing/maintaining recommended practices for securing ICS network architecture(s) for the water sector
- Develop cyber response protocol template
- ICS vendors start to implement or increase their cyber security features by 50%
- Identify and implement existing security features built into devices
- Replace default security passcodes

Mid-Term (2009-2011)

- Reduce installation time of ICS patching
  - PLCs, RTUs, and other frameware by 50%
  - HMI, Operating Systems (O/S), and other applications by 99.9%
- System design accommodates restarts when needed
- Develop operator ICS security training program

Long-Term (2011-2018)

- Develop and implement self-defending ICS & infrastructure
- Integrate cyber security into operator certification requirements
- Real-time security state monitoring for intrusions on new and legacy systems will be commercially available

End State (2018)

- Security solutions for legacy systems and new architecture designs and communication methods will be cost effective

2018

Potential Solutions

- Develop tools for security management (e.g., how to respond to and manage an ICS event)
  - Manage automation decision to "manually override" a cyber event
  - Develop and provide ICS event training on incident response procedures and tools
- Develop baseline security requirements defined across system life cycle for fundamental, intermediate, and advanced security posture
- Develop automated security state and response support systems
  - Adapt intrusion protection systems for more robust application to network and host
- Encourage vendors to harden ICS components and test for vulnerabilities
- Develop cost-effective gateway security that includes firewalls, intrusion detection, and anti-virus protection with maximum host impacts that integrates well with water security ICS
- Develop patching technologies that do not impact 24/7 operating systems
- Establish performance metrics

updates on ICS cannot always be implemented on a timely basis because these updates need to be thoroughly tested by the vendor and the utility. ICS outages often must be planned and scheduled days or weeks in advance. Water systems operate 24/7, which means there is no room for error when upgrading/patching an online ICS. The ICS may also require revalidation as part of the update process. Actionable risk mitigation products that owners and operators can easily understand and use are not available. The lack of collaboration between IT and operations further aggravates the change management process.

Potential Solutions

Managing a cyber event includes preparation, detection and analysis, containment, eradication, recovery, and outreach. The industry first must create a cyber response protocol template (i.e., guidance manual) that includes a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an ICS in the water sector. Because of the complexity and multitude of systems, developing a decision-making tool will enable faster response in balancing automation with manual controls during a cyber event. In the long term, automated security state and response support systems should be developed. Also, training must be provided to ensure security templates and management tools are properly prepared and implemented.

The water sector must define baseline security requirements (i.e., fundamental, intermediate, and advanced levels) to establish security functionality, quality, and assurance (i.e., grounds for confidence) of ICS security activities. These activities should be fully integrated into each phase of the system life cycle—initiation, development and acquisition, implementation, operations and maintenance, and disposition.

In the near term, the sector must identify, publish, and disseminate recommended practices, including ones for securing ICS network architectures and for providing physical and cyber security for remote facilities. Water sector vendors should be encouraged to conduct vulnerability assessments at third party facilities. These assessments can expand the understanding of potential ICS weaknesses and the most effective security practices to mitigate them. Assessments can leverage cyber security knowledge to resolve existing vulnerabilities and improve the design and operation of more secure, more resilient, next-generation ICS.

Maintaining system and information integrity assures that sensitive data has not been modified or deleted in an unauthorized or undetected manner. While some security controls exist to address system integrity concerns, they are not appropriate for all ICS applications. Cost-effective gateway security, including firewalls, intrusion detection, and anti-virus protection, must be developed for water sector ICS. These controls should integrate well and have maximum host impacts.

As utilities implement security solutions into their cyber systems, they will need to understand the level of security improvement to justify and reinforce their value to senior leaders, investors, and customers. The sector should establish metrics that measure the security performance of implemented security solutions in order to establish a baseline of performance and measure future progress.

Goal: Partnership and Outreach

Collaborative partnerships will leverages resources and capabilities among utilities, associations, vendors, communities, government organizations, and others in improving the sector's ability to prepare and respond to cyber events. Combining the expertise and perspectives of all facets of the sector ensures that ICS security needs are being met and anticipated from every angle. Additionally, information and cost sharing minimizes the duplication of technology development efforts and maximizes resources to efficiently achieve effective solutions.

Outreach activities are equally important, as they keep industry groups across the nation informed and up-to-date regarding effective strategies and technologies to mitigate infrastructure risk. Workshops, training courses, and recommended practices increase industry members' awareness of security risks to their own systems. Engaging these groups through outreach encourages them to quickly implement new risk mitigation measures and provide input from the field to help guide

future technology development. A steady stream of communication with federal entities and the general public will sustain support for future investments in cyber security.

The future of ICS security depends on government and sector stakeholders (Exhibit 4.6) coming together to work toward common goals. This ongoing collaboration will accelerate and sustain ICS security advances in the individual utilities, the water sector, and the critical infrastructures that rely on a resilient water sector.

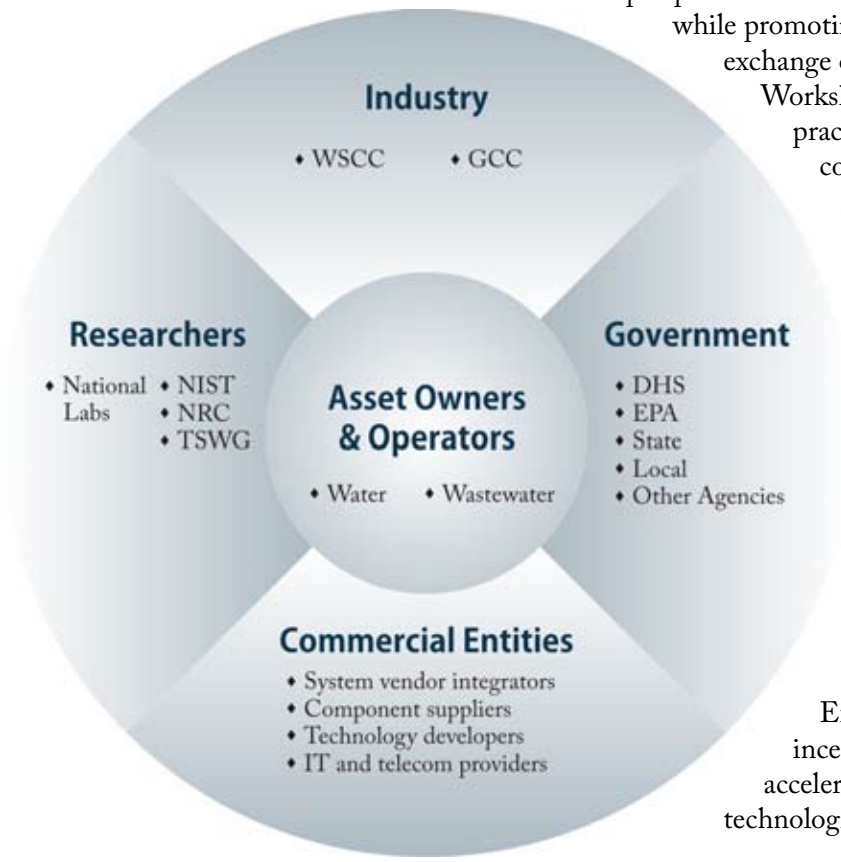
An overview of the challenges, milestones, and potential solutions for conducting partnership and outreach activities in the water sector is shown in Exhibit 4.7.

Challenges

As an emerging requirement for the water sector, ICS risk management is still somewhat isolated. There is a sense that barriers are moved but not broken down. Both industry and government are struggling with how best to initiate ICS security efforts and are still clarifying their respective roles and responsibilities in this emerging area. Although multiple efforts are under way to mitigate ICS risk, effective security-oriented partnerships have been difficult to establish, and poor coordination and insufficient information sharing among stakeholders has created confusion.

Outside of the ICS community, there is a poor understanding of cyber security issues, their implications, and needed actions. It was felt by members at the workshop that federal and utility resources are not adequately focuesd on mitigating ICS risk in the water sector.[2,3] Widespread adoption of ICS security across the entire water sector is challenging due to the voluntary nature of the effort.

Exhibit 4.6 Key Stakeholder Groups and Sample Members



Potential Solutions

In the near-term, the water sector should conduct national workshops with government and sector stakeholders. The contacts and relationships developed during these workshops will serve as a valuable resource in understanding the diverse perspectives on how to achieve common goals, while promoting close cooperation and exchange of ICS security information. Workshops focused on recommended practices will provide a forum for continuous improvement and facilitate widespread adoption of these practices. Additionally, ICS security training should be conducted for employees and contractors.

Establishing and reinforcing a life-cycle investment and framework for ICS security requires an elevated awareness of ICS security risk within the water sector, across critical infrastructures, and among vendor, commercial, and government partners. Effective Federal and state incentives should be developed to accelerate investment in secure ICS technologies and practices. Industry

Exhibit 4.7 Strategies for Conducting Partnership and Outreach

Goal — Partnership and Outreach

Challenges

- Differing view points on how to implement sector partnerships
- Federal and utility resources are not adequately focused on mitigating ICS risk in the water sector
- Difficult to fully implement industrial control systems (ICS) risk mitigation measures across entire water sector on a voluntary basis

Milestones

2008

Near-Term (2008-2009)

- Develop effective federal and state incentives to accelerate investment in secure ICS technologies and practices
- Increase ICS security awareness within the water sector, across critical infrastructure sectors, and with vendor and commercial partners
- Develop essential body of ICS security knowledge for information sharing

Mid-Term (2009-2011)

- Adopt recommended practices for ICS security in the water sector
- Develop public communication channels to increase confidence in water sector efforts to prevent or minimize impacts from a cyber event

Long-Term (2011-2018)

- Establish life cycle investment and framework for ICS security
- Government provides and maintains ICS threat support
- Identify, understand, and disseminate timely ICS risk information within the sector and among its partners

End State (2018)

- Water asset owners and operators will work collaboratively with government and sector stakeholders to accelerate security advances

2018

Potential Solutions

- Conduct national workshops on ICS security within the water sector
- Develop and implement ICS security training for all employees and contractors
- Provide regular updates on water sector ICS security activities to government partners and others (e.g., AWWA, AMWA)
- Work with and leverage a federal program to work with water sector owners and operators on ICS security threats and issues
- Establish performance metrics

associations, such as the American Water Works Association and the Association of Metropolitan Water Agencies, will need to update government and others on a regular basis to maintain ICS security investments for the long term. The sector also needs to identify, understand, and disseminate timely ICS risk information within the sector and among its partners. To simplify and expedite the sharing of ICS security threat information, the water sector should work with and leverage a federal program.

Although quantifying levels of awareness or collaboration is not an easy task, the water sector should establish metrics that measure progress in this important area. Metrics could include the percent of utilities that have adopted recommended practices, number of workshops or training seminars held per year, the number of communication products disseminated throughout the sector, and the amount of investment in ICS security.

V. Implementation

The *Roadmap to Secure Control Systems in the Water Sector* 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, this roadmap does focus on what its contributors believe to be a sound framework that addresses the most significant industrial control systems (ICS) challenges within the next ten years. As such, it is intended to guide the planning and implementation of collaborative cyber security programs that will involve asset owners and operators, industry associations, government, commercial entities, and researchers participating in the national effort to improve security in water sector ICS.

Many water sector organizations have begun to work collaboratively with government agencies, other sectors, universities, and national laboratories, to coordinate efforts to address ICS security concerns. Yet, the current level of investment and resources typically falls short of critical needs. By working together to develop this roadmap, the sector has taken its first step in ICS risk management transformation. Exhibit 5.1 outlines the main roadmap implementation steps. These steps are designed to catalyze buy-in with the roadmap, and subsequently launch and manage ICS security projects. Strong leadership, action, and persistence is needed to ensure that important needs receive adequate support and resources. In addition, achieving early successes is important to maintaining momentum generated by the roadmap and convincing asset owners and stakeholders that the ICS security framework can work.

Exhibit 5.1 Roadmap Implementation Process

Socialize Roadmap

While the precise roles of organizations in implementing this roadmap have not yet been determined, these roles will take shape 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.

Roadmap Oversight and Project Coordination

The contributors of 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. However, without a unified structure, it will be difficult to adequately identify, organize, fund, and track the diverse activities and their corresponding benefits. A roadmap working group, such as the Water Sector Security Council Cyber Security Working Group, can provide the required oversight and collaboration to initiate and find resources for projects and activities.

Initiate and Implement New Activities

The water sector must clearly define the desired outcomes, resources, and capabilities required and how the results will contribute to addressing a particular challenge in the roadmap. Once these

are defined, the working group should evaluate existing activities, identify gaps, and coordinate the development and initiation of new roadmap activities. The working group should also measure progress and track the impact of these activities on achieving roadmap goals.

Sustain Efforts

The risk management planning process must include constant exploration of emerging ICS security capabilities, vulnerabilities, consequences and threats.[4] Because the ICS security concepts described in this roadmap are intentionally broad based, the specific details of assessing risk and employing appropriate risk mitigation strategies will be developed in a technical plan. As the water sector pursues the strategies contained in the roadmap and technical plan, it will continue to review, assess, and adjust the mix of activities that will improve ICS security today and in the future.

VI. For More Information

Seth Johnson
Water Sector Coordinating Council
Cyber Security Working Group Representative
(408) 314-2630
Sethgrp@aol.com

Bruce Larson
Water Sector Coordinating Council
Cyber Security Working Group Representative
BLarson@amwater.com
(609) 922-0804

Dave Edwards
Process Control Systems Forum
Water and Wastewater Representative
(213) 217-5750
dedwards@mwdh2o.com

Kevin Morley
Water Sector Coordinating Council Secretariat
(202) 628-8303
kmorley@awwa.org

Appendix A: Roadmap Process

Initial Water Sector Efforts

This roadmap document was developed by the Water Sector Coordinating Council Cyber Security Working Group. Initial efforts to secure industrial control systems began two years ago with members of the water sector collaborating at the following meetings:

Initial Water Sector Efforts

1/06	Idaho National Laboratory Demonstration, Metropolitan Water District, Los Angeles, CA
3/06	SCADA/IT Security Forum, Los Angeles, CA
6/06	Process Control Systems Forum Meeting, La Jolla, CA
10/06	SCADA/IT Security Forum, Sacramento, CA
3/07	Process Control Systems Forum Meeting, Atlanta, GA
3/07	SCADA/IT Security Summit, Burbank, CA
6/07	SCADA/IT Security Forum, Denver, CO
9/07	Vision Workshop, San Jose, CA
10/07	WSCC Meeting, Washington, DC
12/07	Roadmap Workshop, Washington, DC
1/08	SCADA and Process Control Summit, New Orleans, LA

The roadmap content was developed according to the process shown at the right and described below:

Conduct Workshop

The vision and structure for the roadmap came from 30 executives and ICS experts representing municipal water districts, utilities, private companies, and government agencies who convened on September 20, 2007, in San Jose, California. Led by members of the Water Sector Coordinating Council (WSCC) Cyber Security Working Group (CSWG), the meeting was jointly sponsored by the American Water Works Association (AWWA) and the Department of Homeland Security and hosted by the Santa Clara Water District.

Prepare Meeting Summary Results

The workshop results were published separately in *Cyber Security in the Water Sector: Securing Control Systems Vision Meeting Summary Results,* prepared by Energetics Incorporated, October 19, 2007.[2]

Roadmap Development Process

Brief Water Sector Coordinating Council

On October 30, 2007, results of the workshop were presented to the WSCC.[3] The Council approved support for further development of the roadmap and formally established the WSCC Cyber Security Working Group.

Review Energy Roadmap

The requirements for securing ICS in the water sector are not as rigorous as other sectors, because most water systems are not interconnected and millisecond response is not required. However, similarities do exist and efforts were be made to build on the work already accomplished by the energy sector. The *Roadmap to Secure Control Systems in the Energy Sector* and the vision meeting summary results were used to structure the development of the *Roadmap to Secure Control Systems in the Water Sector*.

Socialize the Vision; Get Buy-In

The vision was shared among members of the water sector to encourage widespread participation in efforts to improve control systems security.

Conduct Workshop

Eight members of the WSCC-CSWG convened on December 20, 2007, at the AWWA in Washington, DC. Based on *Cyber Security in the Water Sector: Securing Control Systems Vision Meeting Summary Results*, the working group synthesized the output within a goal-based strategic framework. The group members also developed a set of milestones, challenges to achieving the milestones, and potential solutions to overcoming the barriers. *A Roadmap for Cyber Security in the Water Sector: Roadmap Meeting Summary Results* was developed by Energetics Incorporated on December 21, 2007, and circulated among the working group for comments.

Prepare, Review, and Publish the Roadmap

The draft roadmap was developed and circulated among all participants from both meetings and other key stakeholders for added insight and clarification. The draft roadmap was presented to the WSCC on February 12, 2008, for comment and approval. The comments of all reviewers have been integrated into this final roadmap document.

Appendix B: References

1. GAO. 2007. Government Accountability Office. Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies (GAO-08-113). Washington, DC. http://www.gao.gov/new.items/d08113.pdf
2. Water Sector Cyber Security Working Group. *Cyber Security in the Water Sector: Securing Control Systems Vision Meeting Summary Results*. Water Sector Control Systems Working Group. October 30, 2007.
3. Water Sector Cyber Security Working Group. *Roadmap for Cyber Security in the Water Sector: Roadmap Meeting Summary Results*. Water Sector Control Systems Working Group. December 22, 2007.
4. DHS. 2006. *DHS National Infrastructure Protection Plan* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
5. Stouffer, Keith, et al. NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security, Second Public Draft*, 2007, http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf
6. GAO. 2007. Government Accountability Office. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain (GAO-07-1036). Washington, DC. http://www.gao.gov/new.items/d071036.pdf
7. ARC Advisory Group. Changing SCADA Systems Market for Water & Wastewater to Exceed $275 Million, October 23, 2007, http://www.arcweb.com/AboutARC/Press/Lists/Posts/AllPosts.aspx
8. Corso, Phaedra S., et al. *Cost of Illness in the 1993 Waterborne Cryptosporidium Outbreak, Milwaukee, Wisconsin*. Emerging Infectious Diseases, April 2003, http://www.cdc.gov/Ncidod/eid/vol9no4/pdfs/02-0417.pdf
9. Gleick, Peter H., et al. T*he World's Water 2006-2007: The Biennial Report on Freshwater Resources*. Pacific Institute for Studies in Development, Environment, and Security. Washington: Island Press, 2006.
10. Nuzzo, Jennerer B. The Biological Threat to U.S. Water Supplies: Toward a National Water Security Policy. Biosecurity and Bioterrorism. Volume 4, Number 2, 2006. Mary Ann Liebert, Inc. http://www.upmc-biosecurity.org/website/resources/publications/2006_orig-articles/2006-06-15-watersecuritypolicy.html
11. CNN. *Sources: Staged cyber attack reveals vulnerability in power grid*. CNN.com/US, September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html
12. McMillan, Robert. IDG News Service. *California Canal Management System Hacked*. PCWorld. December 1, 2007. http://www.pcworld.com/article/id,140190-page,1/article.html
13. SANS NewsBites, Volume X, Issue 5. January 18, 2008. SANS Institute, http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5
14. American Water Works Association Research Foundation (AwwaRF). Actual and Threatened Security Events at Water Utilities. Project 2810. Denver: American Water Works Association Research Foundation; April 2003.
15. Turner, Aaron. U.S. Critical Infrastructure in Serious Jeopardy. CSO Online. http://www2.csoonline.com/exclusives/column.html?CID=32893; Accessed January 7, 2008.
16. Leyden, John. Malware wars: Are hackers on top? The Register, UK. December 5, 2006. http://www.theregister.co.uk/2006/12/05/malware_trends/

17. ASCE, AWWA, WEF. Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System. Water Environment Foundation; December, 2004. http://www.asce.org/static/1/wise.cfm#MonitoringSystem

18. Stewart, W. Kenneth. SFWMD Water Management System (WMS), presentation. Accessed February 4, 2008, http://www.waterweb.org/wis9/pdf/2_Stewart%20WIS9.pdf

19. Ross, Ron, et al. NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, 2007, http://csrc.nist.gov/publications/drafts/800-39/SP-800-39-ipd.pdf

20. Ross, Ron, et al. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, 2007, http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf

21. Synchrony. *Trends in SCADA for Automated Water Systems*. SUNAPSYS; 2001. http://www.sunapsys.com/trends_SCADA.pdf

22. Johnson, Seth and Edwards, Dave. *Why Water and Wastewater Utilities Should be Concerned About Cyber Security*. Journal AWWA. Denver: American Water Works Association; September 2007.

23. DHS and EPA. Water Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. EPA; May 2007. http://www.deq.state.mi.us/documents/deq-wb-wws-Water_SSP_5_21.pdf

24. DOE and DHS. *Roadmap to Secure Control Systems in the Energy Sector*. DOE and DHS. January 2006. http://www.pcsf.org

25. McConnell, J. Michael, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*. Office of the Director of National Intelligence. February 7, 2008. http://www.tsa.gov/assets/pdf/02052008_dni_testimony.pdf

Appendix C: Acronyms

AMWA	Association of Metropolitan Water Agencies
AWWA	American Water Works Association
AwwaRF	Awwa Research Foundation
CDC	Center for Disease Control
CSWG	Cyber Security Working Group
DCS	Distributed Control Systems
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
GAO	U.S. Government Accountability Office
GCC	Government Coordinating Council
HMI	Human Machine Interface
ICS	Industrial Control Systems
IED	Intelligent Electronic Devices
I/O	Input/Output
IT	Information Technology
LAN	Local Area Network
NAWC	National Association of Water Companies
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRC	National Research Council
O/S	Operating System
PLC	Programmable Logic Controllers
RTU	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
TSWG	Technical Support Working Group
WEF	Water Environment Federation
WSCC	Water Sector Coordinating Council
WSSP	Water Sector-Specific Plan