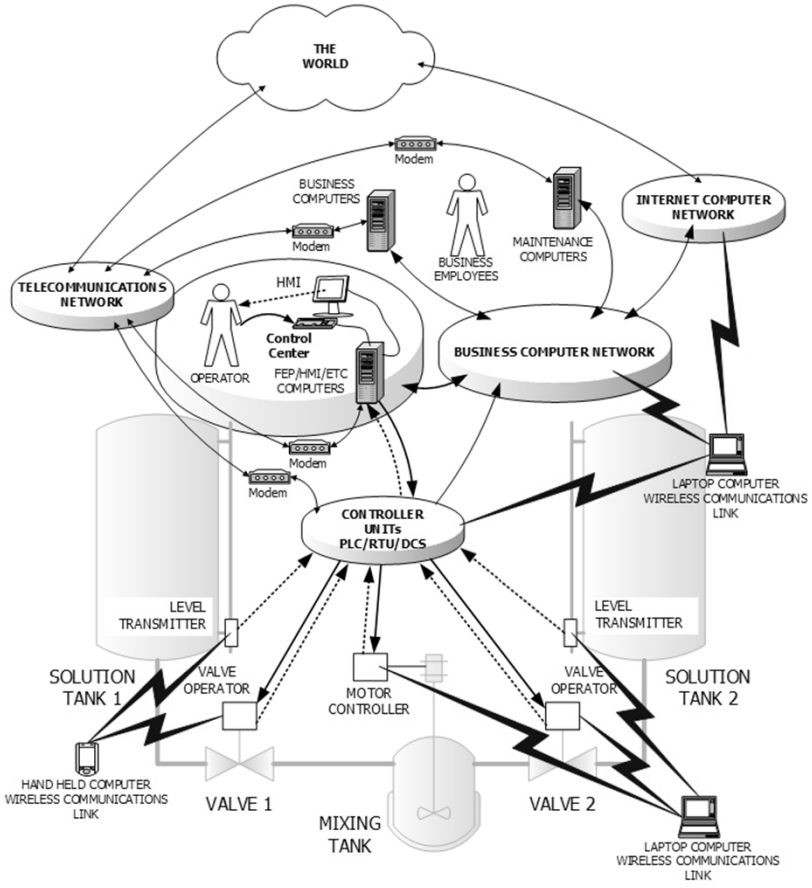
Cybersecurity in the Water Sector

Overview

- Reality of the Threat Environment
- Water Sector Cyber Risk Management
- Key Resources

Connectivity = Exposure



Source: ICS-CERT

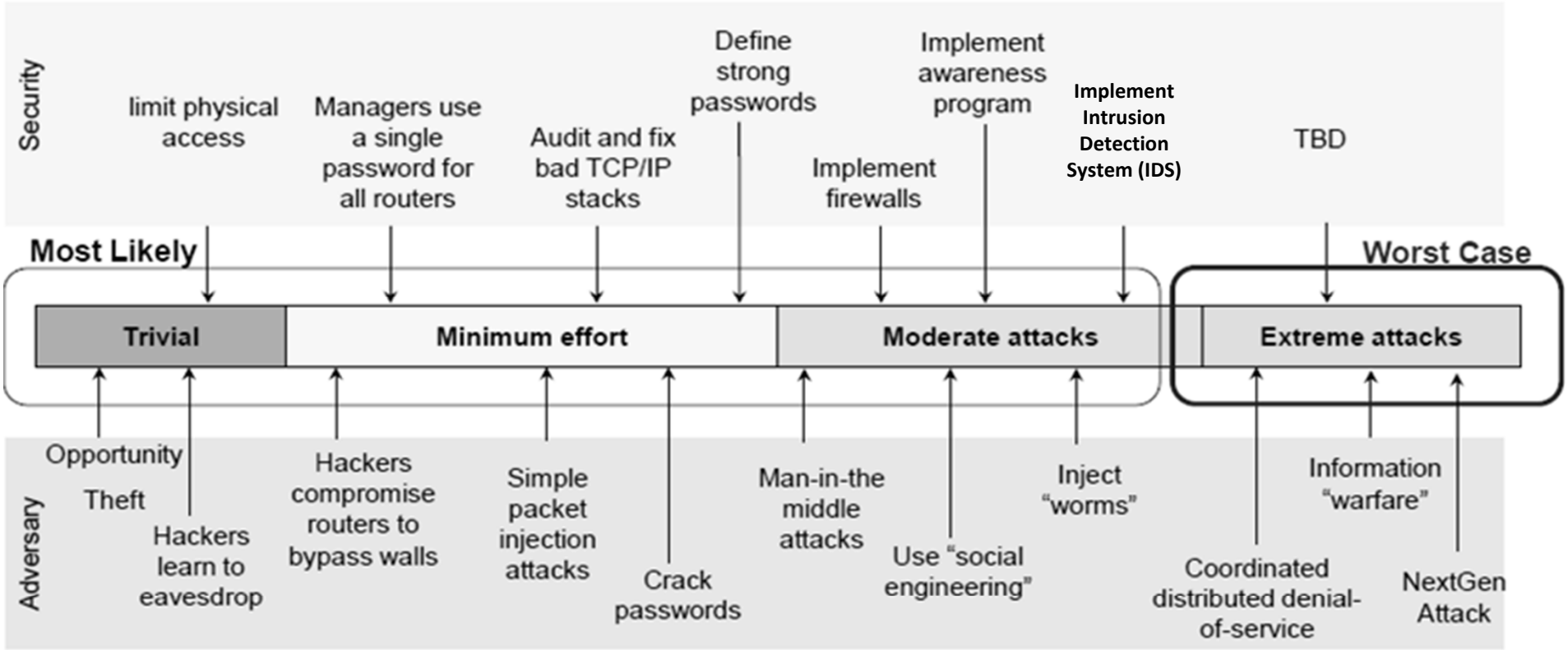
- Process Control Systems
  - SCADA
  - AMR/AMI
  - Telecommunications
  - HVAC
- Enterprise Systems
  - Employee Payroll
  - Service Contracts
  - Customer Billing
  - LIMS etc

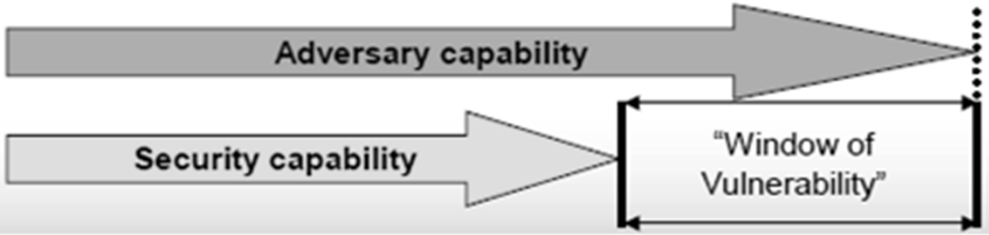
Sobering Reality

- In **60%** of cases, attackers are able to compromise an organization within minutes.#
- Nearly **50%** open E-mails and click on Phishing links within the first hour. #
- ***More than 70%*** of attacks exploited known vulnerabilities with available patches, some dating back to 1999. #
- Forecasted average loss for a breach of 1,000 records is between $52,000 and $87,000. #

2015 Verizon DBIR

Dynamic Threat Environment



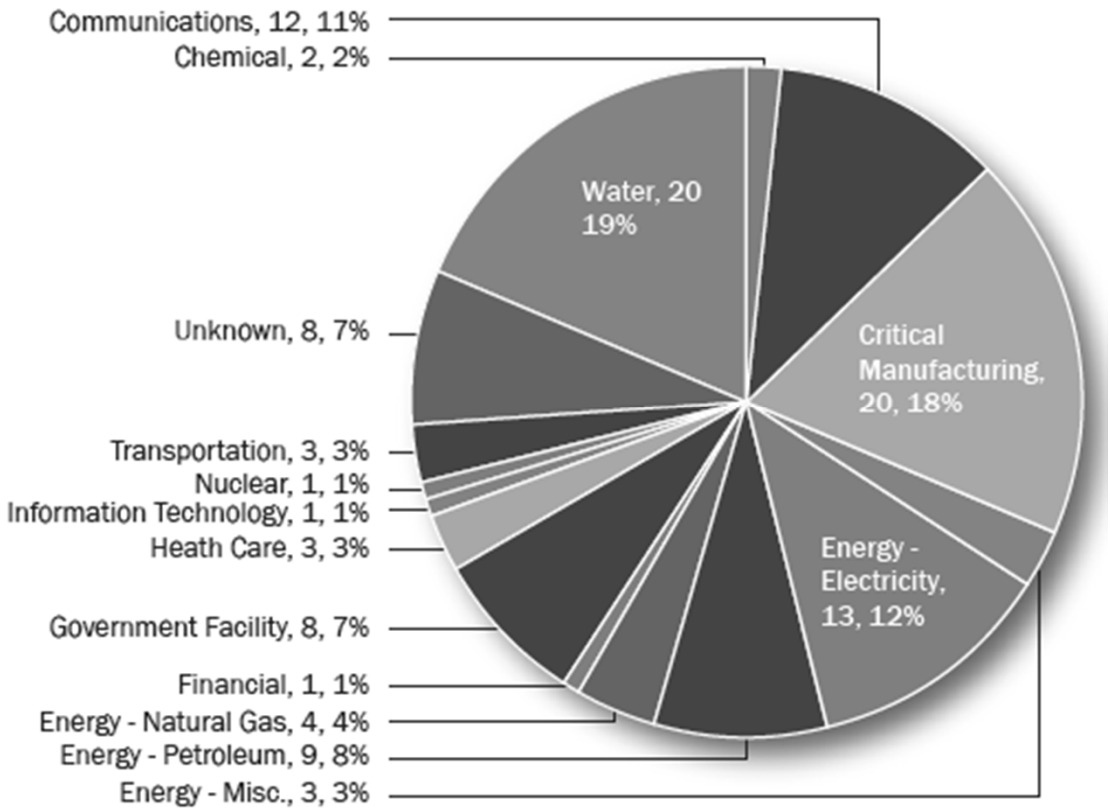


Source: Idaho National Labs

Cyber Threats are Very Real

- Director of National Intelligence confirms multiple directed attacks against control systems for exploitation
- BlackEnergy and Havex malware (2014-15)
- Remotely modified Sacramento River control (2007) < former employee >
- Malware Infection at Harrisburg Water System (2006) < overseas hacker >
- Catastrophic Failure at Taum Sauk Water Storage Dam (2005) < instrumentation / accident >
- Sewage Spill at Maroochy Shire (2000) <disgruntled job applicant >

FY 2015 Mid-Year Incidents



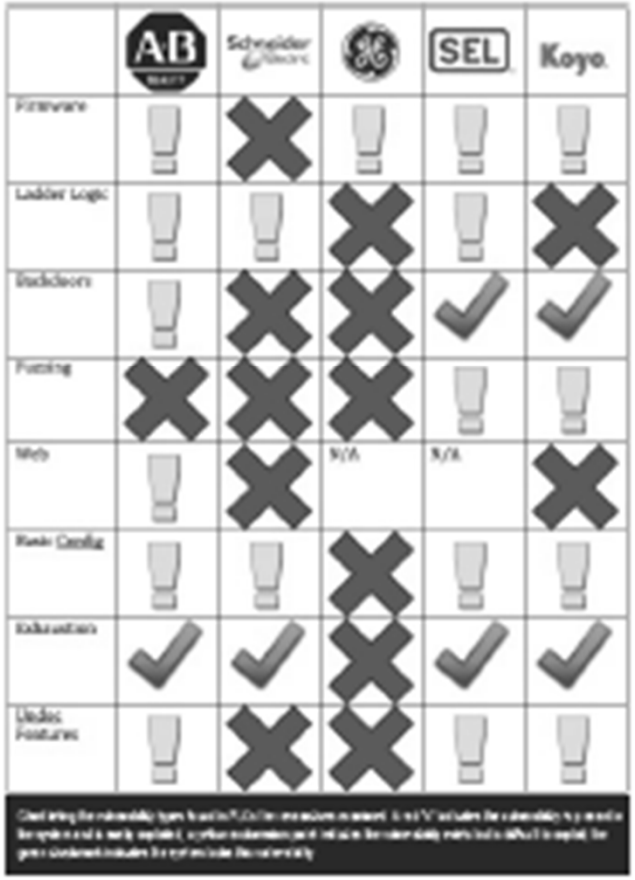
Source: ICS-CERT Monitor, May/June 2015

WIRED

Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software

By Kim Zetter Email Author January 19, 2012 | 7:23 pm | Categories: Hacks and Cracks

The vulnerabilities were found in widely used programmable logic controllers (PLCs) made by General Electric, Rockwell Automation, Schneider Modicon, Koyo Electronics and Schweitzer Engineering Laboratories.



eWEEK.COM

IT Security & Network Security News

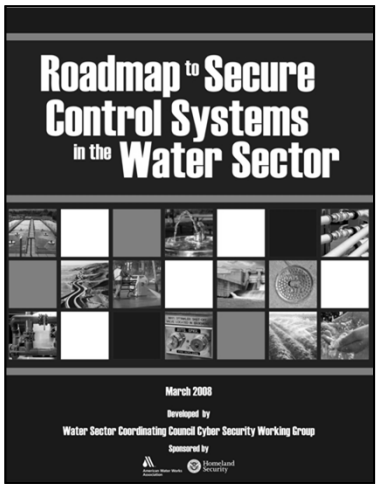
State of SCADA Security Worries Researchers

By: Fahmida Y. Rashid
2012-02-05

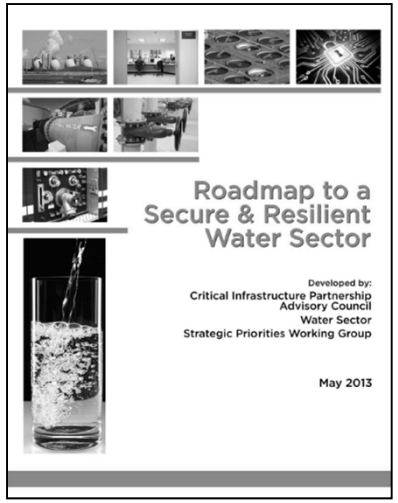
…… locate and map more than 10,000 industrial control systems hooked up to the public Internet, including water and sewage plants. While some may have been test systems, some of them were actually in production. Only 17 percent of the systems found asked remote users for authorization to connect, according to that research.

Water Sector & Cybersecurity

- **Y2K**
- **BT Act 2002**



<u>Critical Milestone</u>
Develop a recommended practices ICS security template for widespread use in the water sector



<u>#1 Priority</u>
Advance the development of sector-specific cybersecurity resources

Standards & Guidance

ANSI/AWWA G430-14: Security Practices for Operation & Management

- Information protection and continuity is a requirement

ANSI/AWWA J100-10: RAMCAP® Standard for Risk & Resilience Management of Water & Wastewater Systems

- Cyber is required threat domain

ANSI/AWWA G440-11: Emergency Preparedness Practices

- Consideration of key business & operating system recovery

Business Continuity Plans for Water Utilities

- Cyber recovery plan is required action item

Process Control System Security Guidance for the Water Sector

- Supports voluntary adoption of NIST Cybersecurity Framework

ANSI/AWWA G430-14

Security Practices for Operations and Management

Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
l) Internal and External Communications
m) Partnerships
n) Verification

National Call to Action

Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013)

NIST Cybersecurity Framework (Feb 2014)

1. Framework Core
2. Framework Profile
3. Framework Implementation Tiers

Voluntary guidance to assist critical infrastructure and business's improve cybersecurity.

But perhaps a bit Abstract

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM)**: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Water Sector Approach

Process Control System Security Guidance for the Water Sector (WITAF #503)

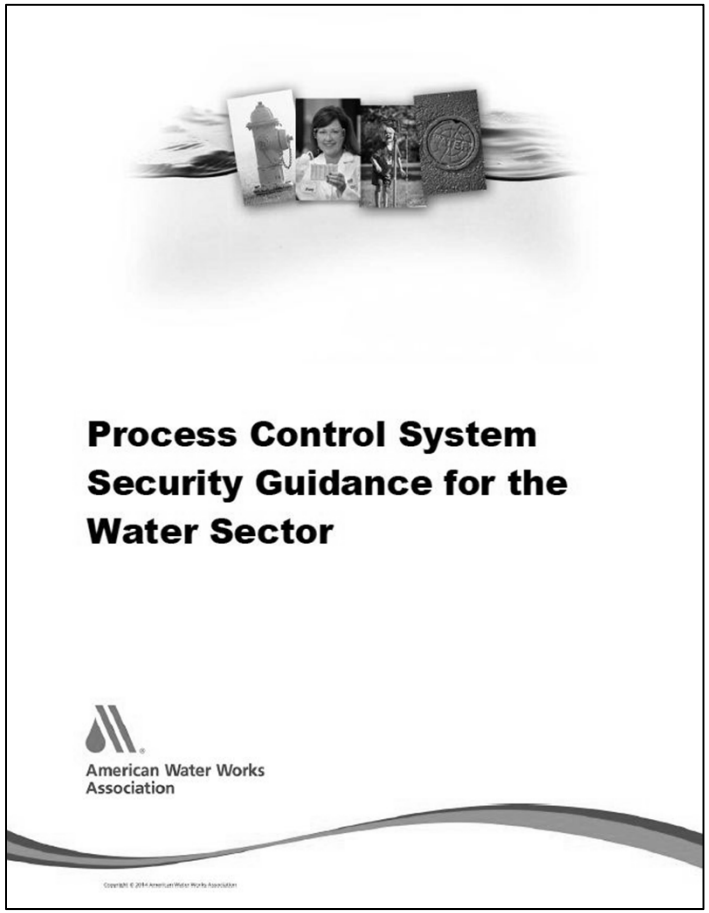
- Develop water sector guidance that provides a consistent and repeatable recommended course of action to reduce vulnerabilities in process control systems.

- Target audience for this resource are water utility general managers, chief information officers and utility directors with oversight and responsibility for process control systems.

- Aligns with sector and national priorities, fulfills need for sector-specific guidance as specified in EO 13636.

- Released February 2014, **www.awwa.org/cybersecurity**

Utility Driven



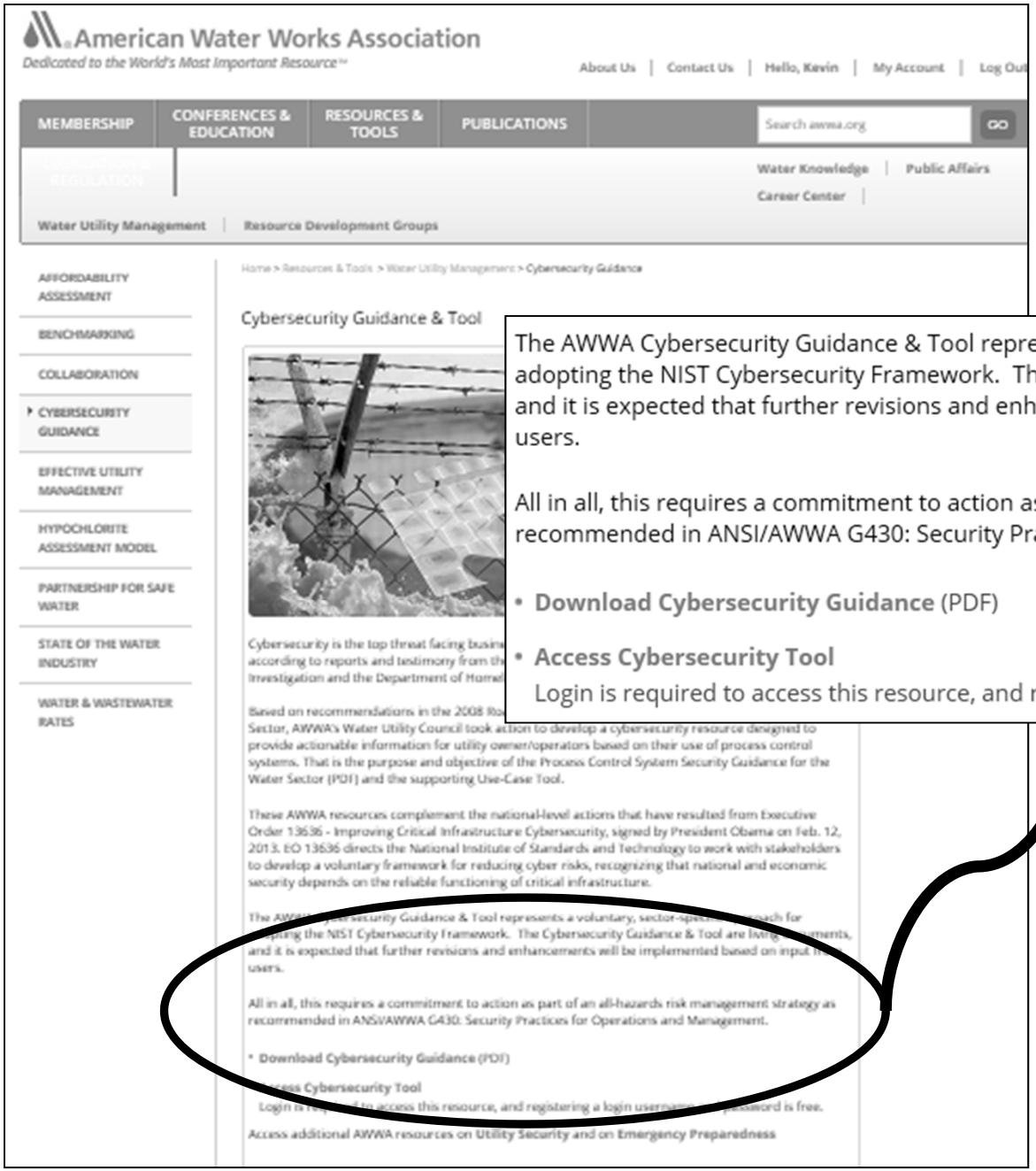
- Organized based on **HOW** the utility uses or operates their process control system
- It does **NOT** evaluate current security profile
- Generates prioritized list of controls that empowers utility to consider appropriate actions to reduce potential vulnerabilities

12 Core Practice Categories

1. Governance & Risk Management
2. Business Continuity & Disaster Recovery
3. Sever & Workstation Hardening
4. Access Control
5. Application Security
6. Encryption
7. Telecomm, Network Security & Architecture
8. Physical Security of PCS Equipment
9. Service Level Agreements (SLA)
10. Operations Security (OPSEC)
11. Education
12. Personnel Security

Use-Case Tool

- 82 Cybersecurity Controls
- Use Cases describe PCS and cyber exposure
- Tool determines which controls apply to selected Use Cases and at which priority (1 – 4)
- Priority 1 – do immediately;
  Priority 4 – important, but not urgent
- ***Tool does not assess current situation***



The AWWA Cybersecurity Guidance & Tool represents a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework. The Cybersecurity Guidance & Tool are living documents, and it is expected that further revisions and enhancements will be implemented based on input from users.

All in all, this requires a commitment to action as part of an all-hazards risk management strategy as recommended in ANSI/AWWA G430: Security Practices for Operations and Management.

- **Download Cybersecurity Guidance** (PDF)
- **Access Cybersecurity Tool**
  Login is required to access this resource, and registering a login username and password is free.

User Access

- [ ] **UA1: Control room system access with control.** Access to system with full read-write capability from "control room" (on-plant, physically secured) location.

- [ ] **UA2: Plant system access with control.** Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).

- [x] **UA3: Remote system access with control.** Access from location outside "control room" environment and located outside the physical perimeter of the facility.

- [ ] **UA4: Remote system access with view-only.** Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility.

- [ ] **UA5: Remote system access with web view.** Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility.

By clicking "Generate Report" you accept AWWA's **terms and conditions**.

GENERATE REPORT

American Water Works Association

CYBERSECURITY REPORT

The following recommended cybersecurity controls represent measures the utility should consider to protect their Process Control System against cyber-attack. The controls have been assigned to four levels of priority based on the user's specific environment as defined by the use cases selected.

Priority 1 controls represent the minimum level of acceptable security for SCADA/PCS. If not already in place, these controls should be implemented immediately.

Priority 2 controls have the potential to provide a significant and immediate increase in the security of the organization.

Priority 3 controls provide additional security against cybersecurity attack of PCS Systems and lay the foundation for implementation of a managed security system. These controls should be implemented as soon as budget allows.

Priority 4 controls are more complex and provide protection for more sophisticated attacks (which are less common). Many Priority 4 controls are related to policies and procedures; others involve state-of-the-art protection mechanisms.

Selected Use Cases:

Architecture

AR1: Dedicated network. All network and communications infrastructure is dedicated exclusively to SCADA. No connection to enterprise networks.

User Access

UA3: Remote system access with control. Access from location outside "control room" environment and located outside the physical perimeter of the facility.

Recommended Controls:

⊟ PRIORITY 1 CONTROLS

AU-2: Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.

DHS CAT: 2.1 Security Policy

ISO/IEC 27001-27005: Annex A: A.5 Security Policy

AU-3: Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.

ISA 62443-2-1: 4.5 Management Responsibility

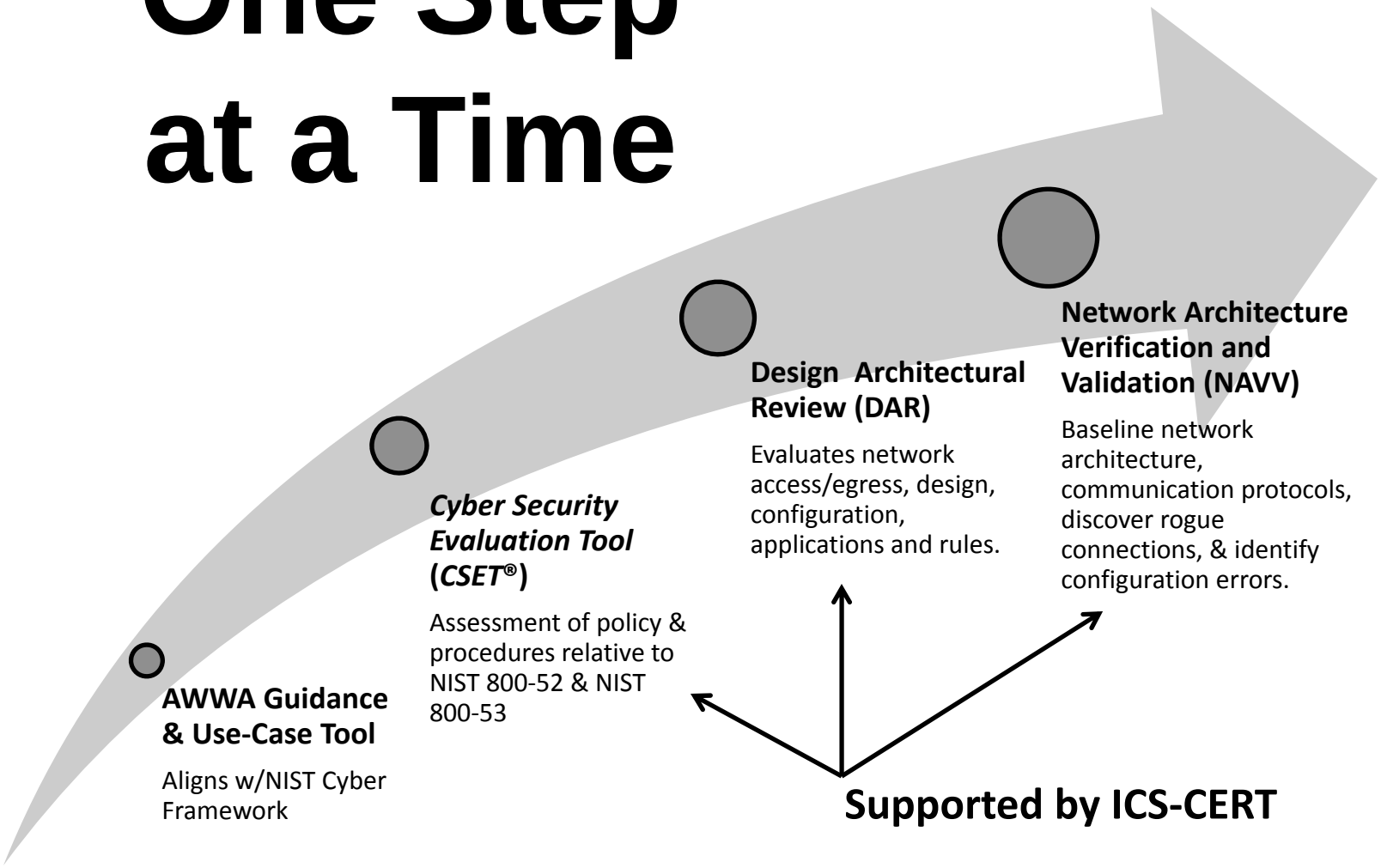
ISO/IEC 27001-27005: 27005 Whole Document

NIST 800-53: Appendix J: AR-1 Governance and Privacy Program

IA-10: Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.

DHS CAT: 12.15.11 Permitted Actions without ID or Authentication

One Step at a Time



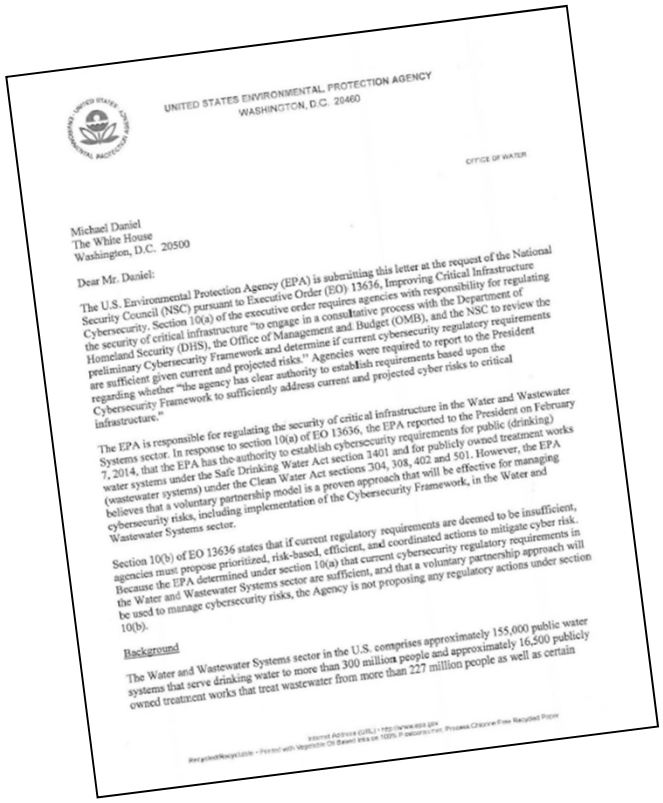
!! Report Incidents !!

ICS-CERT Operations Center

- 1-877-776-7585
- ics-cert@hq.dhs.gov
- **https://ics-cert.us-cert.gov**

Tampering with a Water System is a Federal Offense (42 U.S.C. § 300i-1)

Voluntary Approach



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF WATER

Michael Daniel
The White House
Washington, D.C. 20500

Dear Mr. Daniel:

The U.S. Environmental Protection Agency (EPA) is submitting this letter at the request of the National Security Council (NSC) pursuant to Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. Section 10(a) of the executive order requires agencies with responsibility for regulating the security of critical infrastructure "to engage in a consultative process with the Department of Homeland Security (DHS), the Office of Management and Budget (OMB), and the NSC to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks." Agencies were required to report to the President regarding whether "the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure."

The EPA is responsible for regulating the security of critical infrastructure in the Water and Wastewater Systems sector. In response to section 10(a) of EO 13636, the EPA reported to the President on February 7, 2014, that the EPA has the authority to establish cybersecurity requirements for public (drinking) water systems under the Safe Drinking Water Act section 1401 and for publicly owned treatment works (wastewater systems) under the Clean Water Act sections 304, 308, 402 and 501. However, the EPA believes that a voluntary partnership model is a proven approach that will be effective for managing cybersecurity risks, including implementation of the Cybersecurity Framework, in the Water and Wastewater Systems sector.

Section 10(b) of EO 13636 states that if current regulatory requirements are deemed to be insufficient, agencies must propose prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risk. Because the EPA determined under section 10(a) that current cybersecurity regulatory requirements in the Water and Wastewater Systems sector are sufficient, and that a voluntary partnership approach will be used to manage cybersecurity risks, the Agency is not proposing any regulatory actions under section 10(b).

Background

The Water and Wastewater Systems sector in the U.S. comprises approximately 155,000 public water systems that serve drinking water to more than 300 million people and approximately 16,500 publicly owned treatment works that treat wastewater from more than 227 million people as well as certain

….American Water Works Association has issued "Process Control System Security Guidance for the Water Sector" and a supporting "Use-Case Tool." …. **This tool is serving as implementation guidance for the Cybersecurity Framework in the Water and Wastewater Systems sector.**

- USEPA, May 2014

?? Questions ??

Kevin M. Morley, Ph.D.
Security & Preparedness Program Manager
AWWA – Government Affairs
202-628-8303 or kmorley@awwa.org

www.awwa.org/CYBERSECURITY