Cybersecurity in the Water Sector
Overview

• Reality of the Threat Environment
• Water Sector Cyber Risk Management
• Key Resources
Connectivity = Exposure

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

Source: ICS-CERT
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**.
Dynamic Threat Environment

Implement Intrusion Detection System (IDS)

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
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.

...... 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

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

#1 Priority
Advance the development of sector-specific cybersecurity resources
Standards & Guidance

  – 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

  – 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

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify (ID)</strong></td>
<td><strong>Asset Management (ID.AM):</strong> 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.</td>
<td><strong>ID.AM-1:</strong> Physical devices and systems within the organization are inventoried</td>
<td>• CCS CSC 1&lt;br&gt;• COBIT 5 BAI09.01, BAI09.02&lt;br&gt;• ISA 62443-2-1:2009 4.2.3.4&lt;br&gt;• ISA 62443-3-3:2013 SR 7.8&lt;br&gt;• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2&lt;br&gt;• NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ID.AM-2:</strong> Software platforms and applications within the organization are inventoried</td>
<td>• CCS CSC 2&lt;br&gt;• COBIT 5 BAI09.01, BAI09.02, BAI09.05&lt;br&gt;• ISA 62443-2-1:2009 4.2.3.4&lt;br&gt;• ISA 62443-3-3:2013 SR 7.8&lt;br&gt;• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2&lt;br&gt;• NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ID.AM-3:</strong> Organizational communication and data flows are mapped</td>
<td>• CCS CSC 1&lt;br&gt;• COBIT 5 DSS05.02&lt;br&gt;• ISA 62443-2-1:2009 4.2.3.4&lt;br&gt;• ISO/IEC 27001:2013 A.13.2.1&lt;br&gt;• NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ID.AM-4:</strong> External information systems are cataloged</td>
<td>• COBIT 5 APO02.02&lt;br&gt;• ISO/IEC 27001:2013 A.11.2.6&lt;br&gt;• NIST SP 800-53 Rev. 4 AC-20, SA-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ID.AM-5:</strong> Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value</td>
<td>• COBIT 5 APO03.03, APO03.04, BAI09.02&lt;br&gt;• ISA 62443-2-1:2009 4.2.3.6&lt;br&gt;• ISO/IEC 27001:2013 A.8.2.1&lt;br&gt;• NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ID.AM-6:</strong> Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</td>
<td>• COBIT 5 APO01.02, DSS05.03&lt;br&gt;• ISA 62443-2-1:2009 4.3.2.3.3&lt;br&gt;• ISO/IEC 27001:2013 A.8.1.1</td>
</tr>
</tbody>
</table>
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. Server & 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).

- **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.
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:

PRIORITIZED 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


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

AWWA Guidance & Use-Case Tool
Aligns w/NIST Cyber Framework

Cyber Security Evaluation Tool (CSET®)
Assessment of policy & procedures relative to NIST 800-52 & NIST 800-53

Design Architectural Review (DAR)
Evaluates network access/egress, design, configuration, applications and rules.

Network Architecture Verification and Validation (NAVV)
Baseline network architecture, communication protocols, discover rogue connections, & identify configuration errors.

Supported by ICS-CERT
!! Report Incidents !!

ICS-CERT Operations Center
• 1-877-776-7585
• ics-cert@hq.dhs.gov
• [https://ics-cert.us-cert.gov](https://ics-cert.us-cert.gov)

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

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