September 10, 2014

Process Control System Security Guidance for the Water Sector

EMA

Philip Gaberdiel, P.E.
Principal Consultant

WEAT

Presentation Agenda

1. Background
2. PCS Cybersecurity Guidance

SECTION 1

Background

What is the Problem?

Finding

There is no lack of cybersecurity guidance …..[but] given the plethora of guidance available**, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture.**

Recommendation

Developing a better understanding of the available guidance and best practices would help both federal and private-sector decision-makers coordinate protection of critical cyber-reliant assets.

Source: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use, GAO-12-92 (http://www.gao.gov/assets/590/587529.pdf)

Moving Forward

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

- NIST led development of a ***Cybersecurity Framework***
  - a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.
- Cybersecurity Framework (Version 1.0) was released on February 12, 2014
- NIST will solicit comments on Framework in the near future

Water Sector Approach

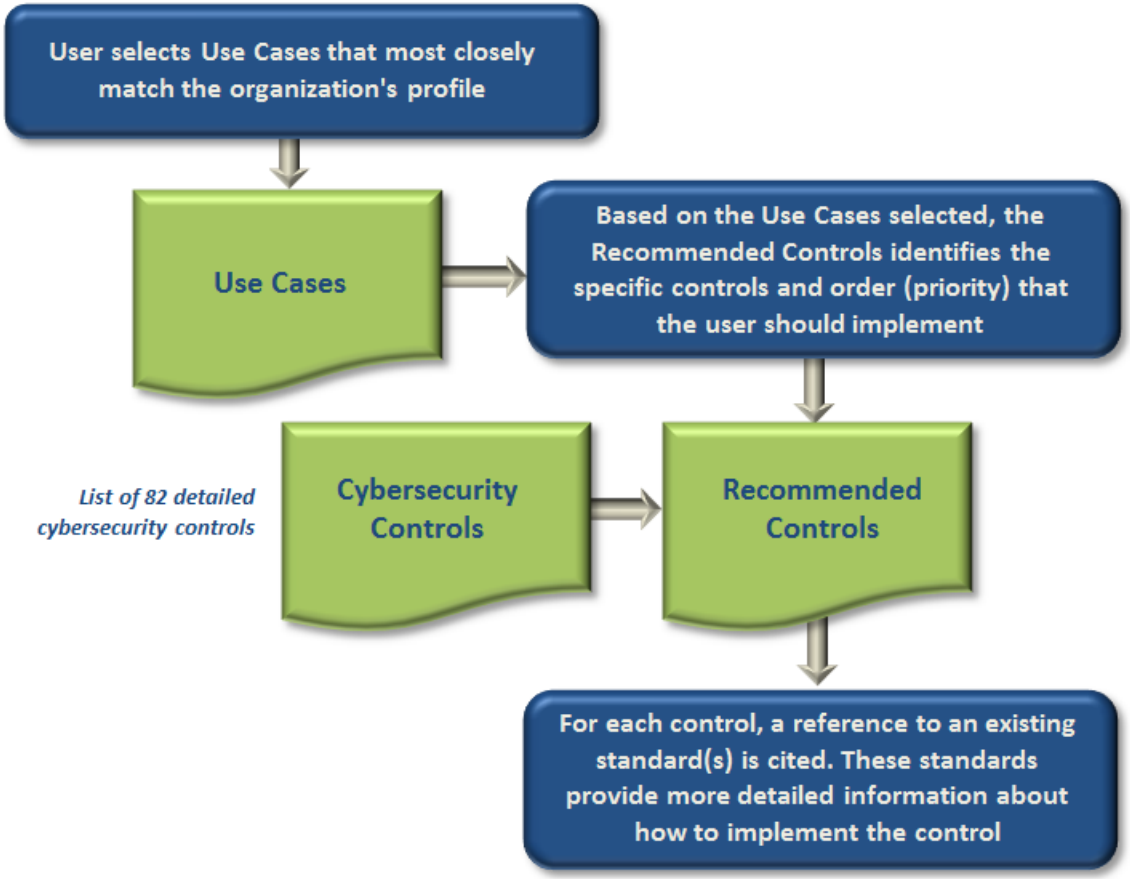
AWWA WITAF Project #503

- 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.
- Project team led by EMA and included SME panel of utility representatives, vendors, consultants, Federal agencies
- Aligns with sector and national priorities, fulfills need for sector-specific guidance as specified in EO 13636. Consistent with NIST Framework.
- Release of web-based Cybersecurity Guidance tool on February 12, 2014

SECTION 2

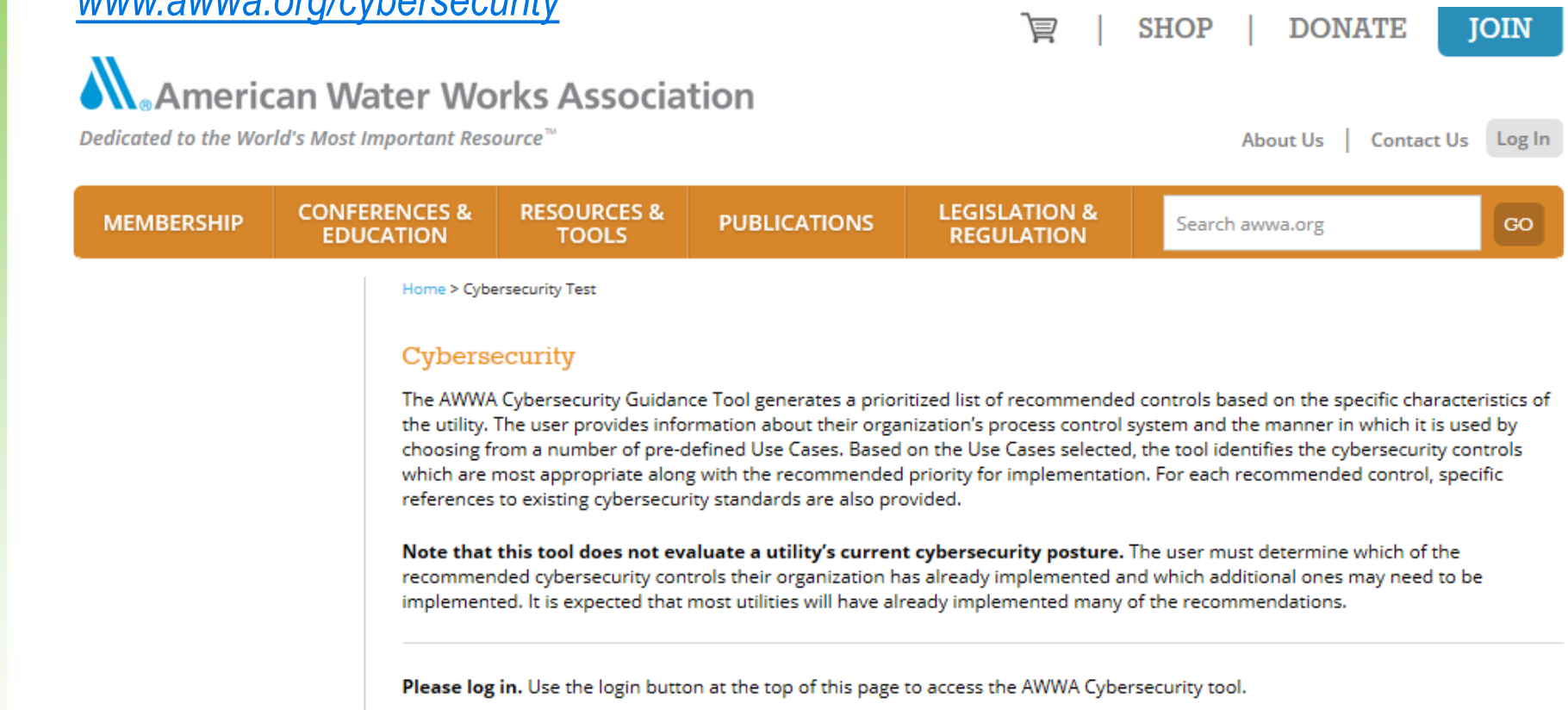
PCS Cybersecurity Guidance

PCS Cybersecurity Guidance



Log-In

www.awwa.org/cybersecurity



AWWA membership is not required to use the Guidance tool

Select Use Cases

Cybersecurity

A use case is an elemental pattern of behavior as described by the user of a system. The use cases presented in the AWWA Cybersecurity Guidance Tool are intended to reflect the manner in which a user's Process Control System is configured and/or the manner in which the organization utilizes the Process Control System. The operational characteristics associated with each use case represent different types and degrees of cybersecurity risk. The guidance tool determines the appropriate cybersecurity controls and priorities based on the use cases selected by the user.

Prior to using the Guidance Tool, the user should review specific information pertaining to the organization's Process Control Systems, including device inventory, network architecture, software functionality, physical facility and plant process architecture. With some utilities, this knowledge is spread among several individuals and/or departments; certain aspects of this detailed knowledge may be held by vendors or external service providers. Conducting a planning meeting with the appropriate resources and stakeholders prior to using the Guidance Tool should be considered.

There is a wide variety of different products and system configurations used for water sector Process Control Systems. As such, some of the use cases provided may not match a user's specific situation exactly. In that case, the user should select the use cases which most closely match the utility's systems and procedures.

Use Cases: (check all that apply)

- ☐ **Select all**

Architecture

- ☐ **AR1: Dedicated network.** All network and communications infrastructure is dedicated exclusively to SCADA. No connection to enterprise networks.
- ☐ **AR2: Shared WAN.** Wide-area network communications infrastructure is shared (controls: physical (media) separation, VPN, VLAN, firewall).
- ☐ **AR3: Shared LAN.** Local-area network communications (within facility) is shared (controls: VLAN, firewall).

Guidance Tool Output

Cybersecurity

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.

As a reminder, the tool does not make any attempt to assess which recommended controls the utility may already have in place. To make effective use of the guidance information provided by the tool, a utility must evaluate each recommendation against the cybersecurity measures, policies, and procedures currently in place and develop a plan of action for addressing those recommended controls not yet implemented.

It should be noted that the Guidance tool also does not provide information about how the recommended controls should be implemented. The tool does provide specific references to existing standards and guidance documents that contain further information about the controls, including a certain amount of implementation details.

Implementing cybersecurity controls requires in-depth knowledge of the affected Process Control System, and the approach must be customized to those specific conditions. Before implementing any cybersecurity related controls which directly affect the Process Control System, a utility should develop a comprehensive plan which details the specific actions to be taken along with an expected timetable. It is important that the project team include resources with the necessary technical skills and system knowledge. The risks associated with implementation of cyber measures should also be fully understood and appreciated by operations and management, and contingency plans should be put in place to address any unintended consequences.

Guidance Tool Output

Selected Use Cases:

Architecture

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

Network Management

NM1: Local network management. Access to configure network infrastructure located in immediate vicinity of user (serial or network).

Program Access

PA1: Outbound messaging. Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.

PA4: Software updates. Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.

PA6: Network monitoring. Automated, non-interactive exchange of network management data (e.g. syslog, SNMP traps, SNMP polling) with system(s) located external to system. (Implies full-time connection.)

PLC Programming and Maintenance

PLC1: Local PLC programming and maintenance. Access to PLC programming and maintenance is local to device (serial or network).

User Access

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).

Guidance Tool Output

⊟ **PRIORITY 1 CONTROLS**

CM-7: Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.

ISO/IEC 27001-27005: 27001 Annex A: A.10.10.2 Monitoring system use

NIST 800-53: Appendix F-CM: CM-11 User-Installed Software

IA-1: Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.

AWWA G430: 4.6 Access Control and Intrusion Detection

NIST 800-82: 6.3.2 Access Countrol

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

IA-12: Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.

ISA 62443-3-3: 9.3 Network Segmentation

NIST 800-53: Appendix F-SC: SC-7 Boundary Protection

NIST 800-82: 5.4 Recommended Defense-in-Depth Architecture

IR-2: A security program established to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.

AWWA G430: 4.4 Up-to-Date Assessment of Risk

DHS CAT: 2.12 Incident Response

NIST 800-61R2: Whole Document

Guidance Tool Output

IA-1: Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.

AWWA G430: 4.6 Access Control and Intrusion Detection

NIST 800-82: 6.3.2 Access Countrol

Industry Adoption

Water Sector Coordinating Council :

"*AWWA's Process Control System Security Guidance for the Water Sector and the supporting Use-Case Tool will serve as the foundation for the water sector's adoption of the NIST Cybersecurity Framework.*"

Since it was released in February, the Cybersecurity Guidance tool has been accessed more than 3,300 times.

Questions

To learn more, please contact:

Philip Gaberdiel, P.E.
Principal Consultant
704.771.5910 or pgaberdiel@ema-inc.com