TETRA TECH

The NIST Cybersecurity Framework

and its relationship to Water & Waste Water

April 25, 2018

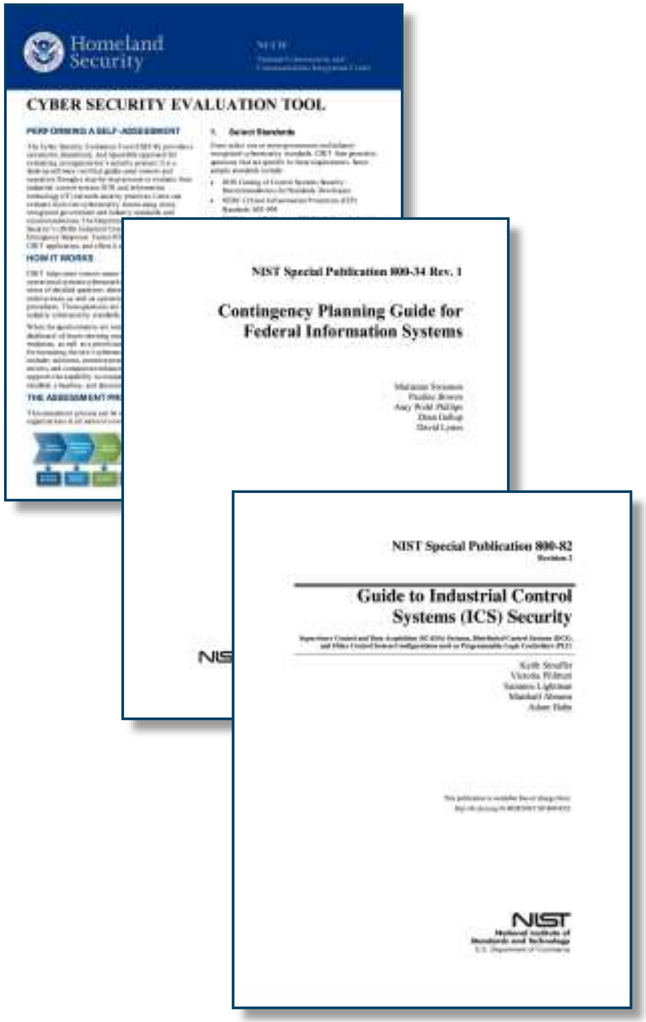
Overview Of This Presentation

- Since its release in early 2014, the NIST Cybersecurity Framework (CSF) has received widespread recognition and uptake by both utility and non-utility sectors.
- Multiple overlapping and seemingly-competing standards and guidance are available.
- This presentation will frame the CSF in relationship to other standards and guidance, and provide context and perspective on its use by water and waste water utilities.

Background

A brief introduction to Internet-connected computing

Cybersecurity Guidance for W/WW



Homeland Security

CYBER SECURITY EVALUATION TOOL

PERFORMING A SELF-ASSESSMENT

1. Select Standards

HOW IT WORKS

THE ASSESSMENT PROCESS

NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- **Pre-2014:**
  - National Institute of Standards and Technology (NIST) SP800-82 Guide to Industrial Control Systems (ICS) Security
  - ISA/IEC-62443 (Formerly ISA-99) Industrial Automation and Control Systems Security
  - WRF CS2SAT and DHS CSET
  - North American Electric Reliability Corporation (NERC) 1300 Critical Infrastructure Protection (CIP) standards

GAO-12-92

- **2011:**
  - The General Accounting Office (GAO) was tasked with identifying the state of cybersecurity within critical industry sectors.
  - Key finding of GAO-12-92 report was that "…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."

EO13636 – Improving Critical Infrastructure

- **February 19, 2013:**
  - Presidential Executive Order (EO) 13636 – Improving Critical Infrastructure – directed the National Institute of Standards and Technology (NIST) to develop a baseline framework to reduce cyber risks to critical infrastructure.

NIST Cybersecurity Framework

- **February 12, 2014:**
  - NIST Cybersecurity Framework developed in response to EO13636.
  - Provides a voluntary framework to identify a “prioritized, flexible, repeatable, performance-based and cost-effective approach” to manage cybersecurity risk.
  - Not specific to any industry.

CSF Characteristics

- Technology neutral.
- Relies on existing standards, guidelines, and practices.
- Provides a set of definitions and mechanisms for organizations to:
    1. Describe their current state of readiness
    2. Describe their target state for readiness
    3. Identify and prioritize improvement based on risk
    4. Evaluate progress toward achieving a desired state
    5. Communicate with internal and external stakeholders on cybersecurity threats and risks – a “Rosetta Stone”.
- The Framework complements, and does not replace, an organization’s risk management process and cybersecurity program.

AWWA Cybersecurity Guidance & Tool

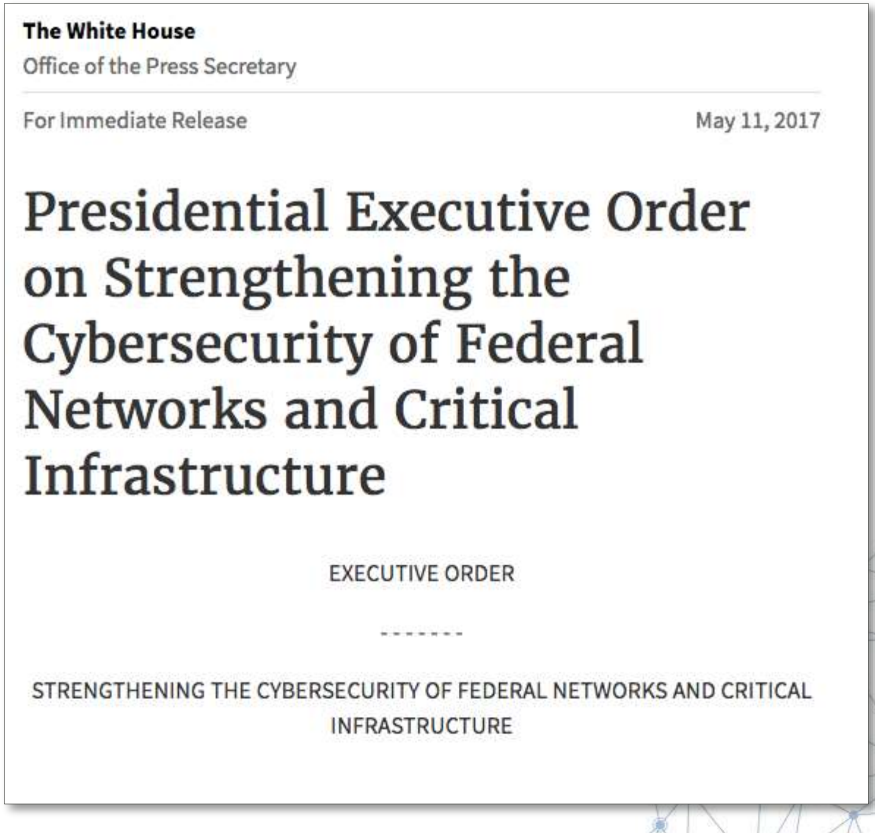
- **February 12, 2014:**
  - The American Water Works Association (AWWA) sponsored Water Industry Technical Action Fund (WITAF) project #503 to develop W/WW-specific guidance to provide *"… a consistent and repeatable recommended course of action to reduce vulnerabilities in process control systems."*
  - The project developed cybersecurity guidance and an online, web-based tool for use by water utility managers. (www.awwa.org/cybersecurity)
  - Provides the W/WW sector with voluntary, sector-specific guidance as called for in EO 13636, aligned with the NIST Cybersecurity Framework.

Relationship Between the NIST CSF and AWWA Cybersecurity Guidance

- Both were developed independently, but the AWWA Guidance is aligned with the NIST CSF.
- The CSF is general and applicable to any industry; the AWWA Guidance is specific to the Water/Waste Water sector and SCADA/ICS.
- The EPA has designated the AWWA Guidance as the sector's official guidance for implementation of the CSF.

Ongoing Evolution of the CSF

- NIST Cybersecurity Framework, Assessment and Auditing Act of 2017 requires NIST to develop outcome-based and quantifiable metrics.
- Executive Order 13800, Strengthening The Cybersecurity Of Federal Networks And Critical Infrastructure, issued on May 11, 2017, calls for all Federal agencies to use the NIST Cybersecurity Framework to guide cybersecurity risk management.



The White House
Office of the Press Secretary

For Immediate Release May 11, 2017

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER

- - - - - - -

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

Implications Executive Order 13800

- The order makes information on the cybersecurity practices of publicly traded companies that own critical infrastructure increasingly known to the public and shareholders.
- Homeland Security to examine existing Federal policies and practices to promote cybersecurity risk management by *publicly traded* critical infrastructure entities.

Overview of the NIST Cybersecurity Framework

CSF Components

- **The CSF consists of three components:**
  1. The Framework Core
  2. Implementation Tiers
  3. Framework Profiles

The Framework Core

- **Identifies sector-agnostic activities and desired outcomes based on existing standards and guidance.**
- **The core incorporates five functions to address these goals:**
  - Identify at-risk assets (systems, equipment, software, hardware and data)
  - Protect assets with appropriate controls
  - Detect cybersecurity anomalies potentially impacting assets
  - Respond to cybersecurity incidents
  - Recover and restore impacted assets
- **The Core comprises the bulk of the CSF, correlating activities and outcomes with established cybersecurity standards and references**

Implementation Tiers

- **Identify the user's current and desired effectiveness of risk management processes. These include:**
  - Partial (Tier 1): Informal, ad-hoc and often reactive.
  - Risk Informed (Tier 2): Approved practices, not fully implemented organization-wide. Cybersecurity awareness, inconsistent or incomplete implementation.
  - Repeatable (Tier 3): Formally approved policies and updated practices. Risk managed organization-wide. Staff has resources to address threats. Share information with partner agencies.
  - Adaptive (Tier 4): Actively reviewed and maintained polices. Continual-improvement process. Risk management a fundamental part of organizational planning. Information is actively shared with partner agencies.
- **Not a maturity model! There is no one "correct" end state.**

Framework Profiles

- Identify current ("as is") and desired ("to be") states.
- Incorporate efforts at the executive, business and operational levels.

The Current State of W/WW Cybersecurity Guidance

Mandates and Drivers

- There is currently no federally-mandated cybersecurity standard for the W/WW sector.
- Individual states are beginning to introduce mandated standards:
  - February 2015: New York Senate passed cybersecurity bills focused on critical infrastructure.
  - March 2016: New Jersey Board of Public Utilities adopted a set of requirements for regulated utilities, including W/WW.
- While the impact of such mandates is still to be determined, it is clear that any future mandates will be far more complex than the existing voluntary measures

Mandated Standards

- Both the NIST CSF and AWWA Guidance provide a *voluntary* framework for development of a cybersecurity compliance program.
- This is in stark contrast to the stringent, mandated compliance standards for the power sector.

NERC Critical Infrastructure Protection (CIP)

- **The North American Electric Reliability Corporation (NERC) developed the Critical Infrastructure Protection (CIP) standards to protect the Bulk Electric System (BES).**
- **While not directly applicable to W/WW, CIP is notable for two reasons:**
    1. It is referenced as a standard by the AWWA Guidance.
    2. It provides a good indicator of what mandated cybersecurity measures will look like should voluntary measures prove inadequate.

NERC CIP v5 Rules

- **11 areas of focus:**

Standard	Focus
CIP-002-5.1	Cyber Security – BES Cyber System Categorization
CIP-003-6	Cyber Security – Security Management Controls
CIP-004-6	Cyber Security – Personnel & Training
CIP-005-5	Cyber Security – Electronic Security Perimeter(s)
CIP-006-6	Cyber Security – Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security – System Security Management
CIP-008-5	Cyber Security – Incident Reporting and Response Planning
CIP-009-6	Cyber Security – Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security – Configuration Change Management, Vulnerability Assessments
CIP-011-2	*Cyber Security – Information Protection*
CIP-014-2	*Physical Security*

Conclusions

Where are we now?

- **The state of cybersecurity readiness varies greatly between and within W/WW utilities.**
- **While some have implemented mature, robust programs, many more are still struggling with the basics.**
  - Many utilities are unaware of available guidance, or confused by seemingly competing initiatives.
  - Guidance varies in how it prioritizes cybersecurity improvement efforts, particularly in identifying the *actual risk* associated with deficiencies.
  - The importance of proactively addressing cybersecurity rather than waiting for a mandate cannot be overstated. Don't play catch up!
  - Boards and management are less likely to be understanding of inadequate preparation in light of highly publicized incidents.
  - The perception of a utility as insecure and potentially unsafe by their customer base is unacceptable.

A Combined Approach for W/WW

- The NIST Cybersecurity Framework provides utilities with a roadmap for identifying and mitigating cybersecurity risks aligned with system criticality.
- Combined with the AWWA Cybersecurity Guidance and Tool, it can provide a mechanism to identify critical SCADA/ICS components, and prioritize efforts to remediate cybersecurity threats to W/WW based on risk.

Process Control System
Security Guida
Water Sector

American Water Works Association

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

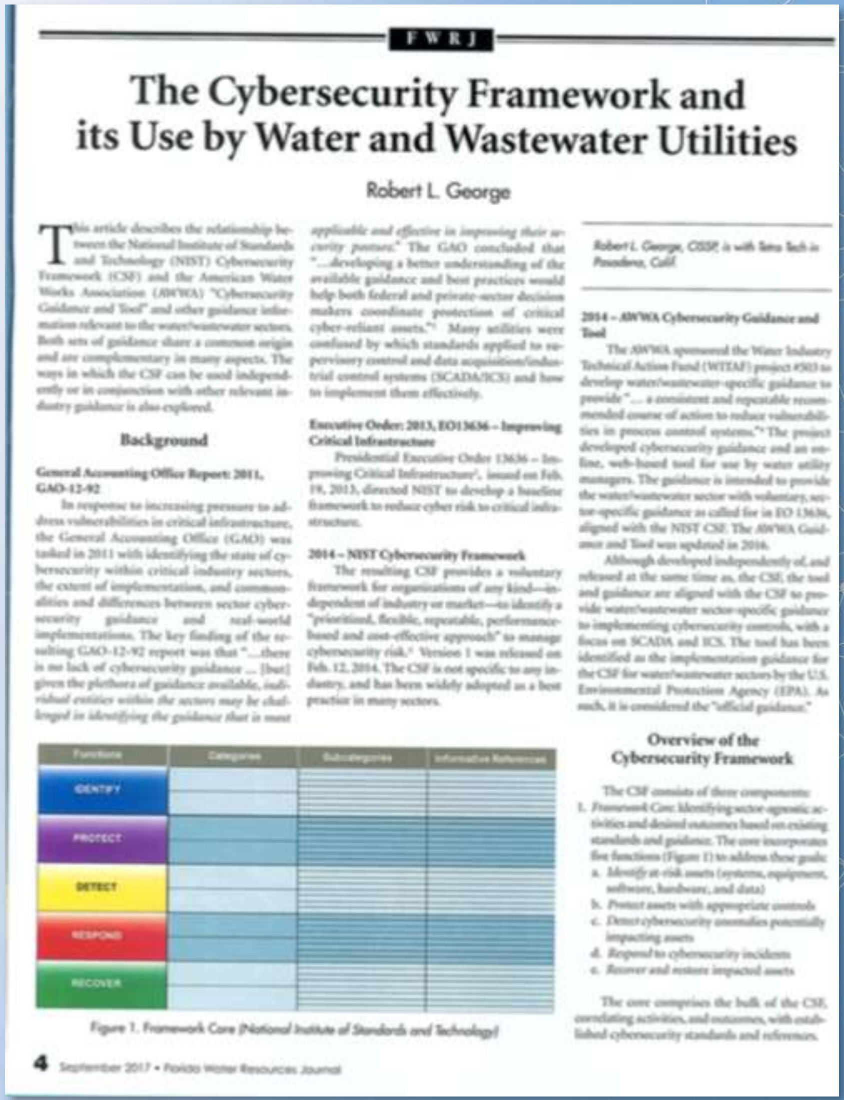
Questions?

Thank You

For more information, please contact:

Bob George, CISSP
bob.george@tetratech.com

The full article is available in the Florida Water Resources Journal, September 2017 issue



FWRJ

The Cybersecurity Framework and its Use by Water and Wastewater Utilities

Robert L. George

This article describes the relationship between the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the American Water Works Association (AWWA) "Cybersecurity Guidance and Tool" and other guidance information relevant to the water/wastewater sectors. Both sets of guidance share a common origin and are complementary in many aspects. The ways in which the CSF can be used independently or in conjunction with other relevant industry guidance is also explored.

Background

General Accounting Office Report: 2011, GAO-12-92

In response to increasing pressure to address vulnerabilities in critical infrastructure, the General Accounting Office (GAO) was tasked in 2011 with identifying the state of cybersecurity within critical industry sectors, the extent of implementation, and commonalities and differences between sector cybersecurity guidance and real-world implementations. The key finding of the resulting GAO-12-92 report was that "...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.*" The GAO concluded that "...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."[1] Many utilities were confused by which standards applied to supervisory control and data acquisition/industrial control systems (SCADA/ICS) and how to implement them effectively.

Executive Order: 2013, EO13636 – Improving Critical Infrastructure

Presidential Executive Order 13636 – Improving Critical Infrastructure[2], issued on Feb. 19, 2013, directed NIST to develop a baseline framework to reduce cyber risk to critical infrastructure.

2014 – NIST Cybersecurity Framework

The resulting CSF provides a voluntary framework for organizations of any kind—independent of industry or market—to identify a "prioritized, flexible, repeatable, performance-based and cost-effective approach" to manage cybersecurity risk.[3] Version 1 was released on Feb. 12, 2014. The CSF is not specific to any industry, and has been widely adopted as a best practice in many sectors.

Robert L. George, CISSP, is with Tetra Tech in Pasadena, Calif.

2014 – AWWA Cybersecurity Guidance and Tool

The AWWA sponsored the Water Industry Technical Action Fund (WITAF) project #503 to develop water/wastewater-specific guidance to provide "... a consistent and repeatable recommended course of action to reduce vulnerabilities in process control systems."[4] The project developed cybersecurity guidance and an online, web-based tool for use by water utility managers. The guidance is intended to provide the water/wastewater sector with voluntary, sector-specific guidance as called for in EO 13636, aligned with the NIST CSF. The AWWA Guidance and Tool was updated in 2016.

Although developed independently of, and released at the same time as, the CSF, the tool and guidance are aligned with the CSF to provide water/wastewater sector-specific guidance to implementing cybersecurity controls, with a focus on SCADA and ICS. The tool has been identified as the implementation guidance for the CSF for water/wastewater sectors by the U.S. Environmental Protection Agency (EPA). As such, it is considered the "official guidance."

Overview of the Cybersecurity Framework

The CSF consists of three components:

1. *Framework Core:* Identifying sector-agnostic activities and desired outcomes based on existing standards and guidance. The core incorporates five functions (Figure 1) to address these goals:
   a. *Identify at-risk assets (systems, equipment, software, hardware, and data)*
   b. *Protect assets with appropriate controls*
   c. *Detect cybersecurity anomalies potentially impacting assets*
   d. *Respond to cybersecurity incidents*
   e. *Recover and restore impacted assets*

The core comprises the bulk of the CSF, correlating activities, and outcomes, with established cybersecurity standards and references.

Figure 1. Framework Core *(National Institute of Standards and Technology)*