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.

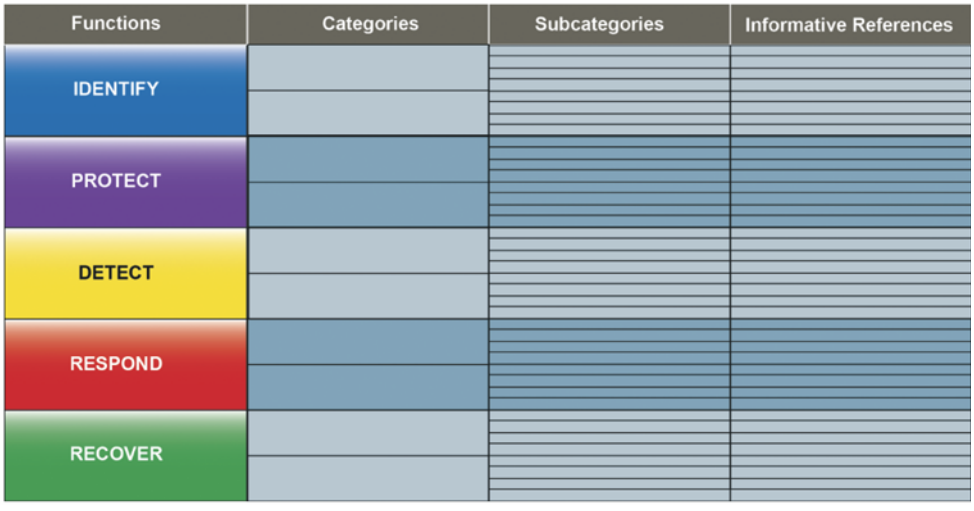

Figure 1. Framework Core *(National Institute of Standards and Technology)*

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.

2. *Implementation Tiers.* Identifying the user's current and desired effectiveness of risk management processes. These include:
   a. *Partial (Tier 1)* based on informal, ad hoc, and often reactive management practices, with limited understanding of actual risks and coordination with other agencies.
   b *Risk Informed (Tier 2)* based on approved practices that are not fully implemented organizationwide, with cybersecurity awareness, but inconsistent or incomplete implementation. Cooperation with other agencies is not formalized or structured.
   c. *Repeatable (Tier 3)* based on formally approved policies and updated practices. Risk is managed organizationwide, and staff has adequate resources to address threats. The organization shares information with partner agencies.
   d. *Adaptive (Tier 4)* based on actively reviewed and maintained polices through a continual-improvement process. Risk management is a fundamental part of organizational planning, and information is actively shared with partner agencies.
3. *Framework Profiles.* Identifying current ("as is") and desired ("to be") states, incorporating efforts at the executive, business, and operational levels (Figure 2).

The CSF provides an approach to managing cybersecurity based on risk, with emphasis on those systems and activities with the greatest potential financial, operational, and safety impacts. It provides a utility with a method of clearly defining its tolerance for risk, and to guide policy and planning efforts.

Current State of Cybersecurity Guidance for Water and Wastewater

While there is currently no federally mandated cybersecurity standard for water/wastewater, individual states are beginning to introduce legislation that effectively transforms voluntary guidelines into mandated standards.

- In February 2015, the New York Senate passed a suite of cybersecurity bills focused on critical infrastructure, including S3405[5], which implements a review and reporting process for key state agencies, and S3407[6], which introduces information-sharing protocols. The bill implements a "consultative process," requiring public and private entities to participate.
- In March 2016, the New Jersey Board of Public Utilities adopted a set of requirements for regulated utilities, including water/wastewater.[7] All utilities are to implement a series of requirements, including a cybersecurity program, to define and implement cyber risk management.

While the impact of these and similar mandates is still to be determined, it is clear that, when mandates arrive, they will be far more onerous and cumbersome to implement than the voluntary measures that preceded them. These efforts mandate implementation of cybersecurity programs that closely resemble the most rigid mandatory rules for utilities: the North American Electrical Reliability Corp. (NERC) critical infrastructure protection (CIP) body of standards.

Contrast With Other Sectors

Both the CSF and AWWA Guidance and Tool 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.

2008 – North American Reliability Corp. Critical Infrastructure Protection

The NERC developed CIP standards to protect the Bulk Electric System (BES) against cybersecurity threats to grid stability.[8] While not directly applicable to water/wastewater, CIP is notable for two reasons:

1. It is referenced as a standard by the AWWA Guidance and Tool.
2. It provides a good indicator of what mandated cybersecurity measures will look like

Continued on page 6

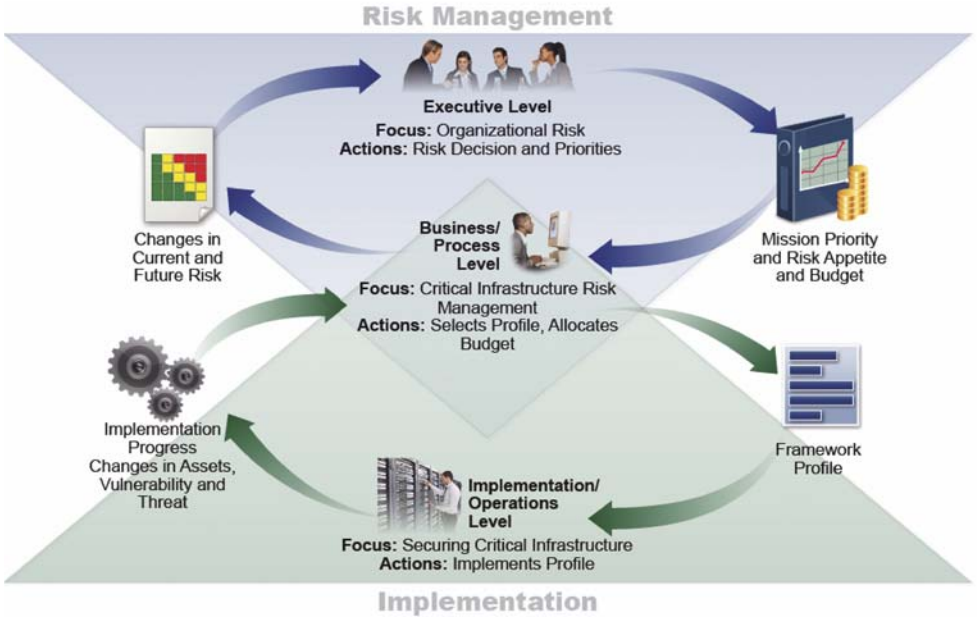

Figure 2. Executive, Business, and Operations Level Efforts
(National Institute of Standards and Technology)

Table 1. North American Electrical Reliability Corp. Critical Infrastructure Protection Version 5 Rules

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 and 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

Continued from page 5

should voluntary measures prove inadequate.

The latest iteration, NERC CIP Version 5, defines a cyber asset as an asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or nonoperation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES."[9]

All BES cyberassets are classified as high, medium, or low impact using a "bright-line" approach to identify assets subject to CIP requirements. A bright-line rule (or bright-line test) is defined as "a clearly defined rule or standard, composed of objective factors, which leaves little or no room for varying interpretation. The purpose of a bright-line rule is to produce predictable and consistent results in its application." [10]

Version 5 focuses on qualitative assessment of internal controls, rather than measurement against requirements. The CIP standards are applied to address risk that is based on the classification of the asset. While previous iterations tended to focus on quantitative "checklists," Version 5 requires a qualitative evaluation of the overall effectiveness of controls.

While a detailed analysis of the NERC CIP standards can (and does) fill volumes, a few characteristics are noteworthy for water/wastewater customers:

- They are comprehensive, encompassing both policy and technical topics.
- They require continuous review and update, with refreshes every 15 months.
- They are expanding and growing in scope, with physical security being added in Version 5.
- Most impacted utilities employ multiple individuals dedicated to CIP compliance.

Table 1 summarizes the CIP Version 5 rules as of mid-2016.

Guidance Versus Standards

It is important to distinguish between guidance and standards when referring to cybersecurity references. The following working definitions are used here:

- *Standards* define methods, technologies, and/or architectures to be used to secure a system in specific circumstances. There are many cybersecurity standards produced by different standards bodies, with each focusing on the concerns of a particular industry or market. In many cases, standards from different bodies within a single industry overlap. While most standards within an industry recommend similar practices, variations in terminology and approach, as well as differences between industries, can cause confusion.
- *Guidance* provides recommendations for standards to be applied to a specific industry or setting. Guidance does not specify practices, but typically references one or more standards or bodies of standards applicable to a specific industry.

Cybersecurity Standards

All of the current water/wastewater cybersecurity guidance refers to a number of general and industry-specific standards for detailed implementation recommendations. Many utilities are familiar with some of these by other, older names. Commonly referenced standards include:

- ISA/IEC-62443 (Formerly ISA-99) Industrial Automation and Control Systems Security, including TR99.00.02 (2007)
- NIST SP800-82 Rev. 1 Guide to Industrial Control Systems (ICS) Security (2013)
- NERC 1300 Critical Infrastructure Protection (CIP) standards CIP-002 – CIP-009 (2008)
- NIST SP800-34 Rev. 1 Contingency Planning for Federal Information Systems (2010)
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002 (formerly ISO/IEC 17799) Information technology – Security techniques – Code of practice for information security management.
- NIST SP800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations (2014)
- U.S. Department of Homeland Security (DHS) Recommended Practice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies (2009)
- DHS Catalog of Security Recommendations, the "Catalog of Control Systems Security, Recommendations for Standards Developers," a document developed for the U. S. Department of Homeland Security (DHS).

Conclusions

The state of cybersecurity readiness varies greatly within and among water/wastewater utilities. While some have implemented mature, robust programs, many more are still struggling with the basics, and where to start.

1. While cybersecurity guidance is freely available, many utilities are unaware of it, or confused by seemingly competing initiatives.
2. Guidance varies in how it prioritizes cybersecurity improvement efforts, particularly in identifying the actual risk associated with deficiencies.
3. The importance of proactively addressing cybersecurity, rather than waiting for a

Recent News on the NIST Cybersecurity Framework

- Congressional bill HR 1224 NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, dated Feb. 27, 2017, requires NIST to develop outcome-based and quantifiable metrics. Specific language will be added, including underscoring the need for applying security engineering at the beginning of a system life cycle, building secure systems and components from the start of a project, and applying well-defined security design principles throughout a system's life cycle (see https://www.congress.gov/bill/115th-congress/house-bill/1224).

- 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 (see https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal).

mandate, cannot be overstated. Boards and management are less likely to be understanding of inadequate preparation in light of highly publicized breaches at Target, Home Depot, and other high-profile commercial chains. The perception of a utility as insecure and potentially unsafe by its customer base is unacceptable.

The NIST CSF 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 based on risk.

References

[1] "Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can be Done to Promote its Use." U.S. GAO - http://www.gao.gov/products/GAO-12-9.

[2] "Executive Order: Improving Critical Infrastructure Cybersecurity." https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[3] "NIST Framework for Improving Critical Infrastructure Cybersecurity." https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[4] "AWWA Cybersecurity Guidance and Tool." https://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx.

[5] Senate Bill S3405 - https://www.nysenate.gov/legislation/bills/2009/s3405/amendment/original.

[6] Senate Bill S3407A - https://www.nysenate.gov/legislation/bills/2015/s3407/amendment/a.

[7] Transmission Hub, "New Jersey BPU directs utilities to have cybersecurity program." - http://www.transmissionhub.com/articles/2016/03/new-jersey-bpu-directs-utilities-to-have-cybersecurity-program.html.

[8] NERC United States Mandatory Standards Subject to Enforcement. http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States.

[9] Identifying Critical Cyber Assets - http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf.

[10] Wikipedia "Bright-Line Rule" - https://en.wikipedia.org/wiki/Bright-line_rule.