STRENGTHENING THE CYBER RESILIENCE OF AMERICA'S WATER SYSTEMS: INDUSTRY-LED REGULATORY OPTIONS

Prepared by Paul N. Stockton

for the American Water Works Association

August 27, 2021

STRENGTHENING THE CYBER RESILIENCE OF AMERICA'S WATER SYSTEMS: INDUSTRY-LED REGULATORY OPTIONS

EXECUTIVE SUMMARY

America's water systems are facing increasingly severe cyber threats. A growing number of system operators are responding with new security initiatives and leveraging government and industry cyber recommendations to build cyber resilience though voluntary measures. But very limited mandatory standards exist to ensure progress on a nationwide basis. Given the vital role of water service for public health and safety, the economy, and national security, the intensifying domestic and foreign cyber threats mean that the time has come to establish a stronger regulatory framework to support water sector cyber resilience.

This study proposes options to establish a new sector-led organization to manage the development of mandatory cybersecurity standards and oversee compliance with them. This new approach would have federal oversight that is focused on defining requirements for standards and approval of their use for implementation. The US Environmental Protection Agency (USEPA) would be the principal Federal oversight agency with technical support provided by CISA and DOE given existing cybersecurity expertise. However, the water sector would manage the standards development process and associated implementation, and thereby capitalize on the sector's expertise of water utility operations and governance.

Many water sector associations already provide valuable support to their members on cybersecurity issues. Rather than select one to lead standards development and compliance, this study suggests creating a new entity: a Water Risk & Resilience Organization (WRRO) to serve and represent the perspectives of utilities across the sector. Existing associations and their members are best positioned to reach consensus on how the WRRO should be governed and resourced.

This approach will require legislative action to authorize the oversight function and define scope of coverage for mandatory water utility participation in implementing minimum standards of practice developed by the WRRO. It is essential that the standards of practice developed and selected are scalable and risk-based given the differences in of utility operations across all size categories.

Resourcing this new approach will be critical to successfully supporting the cyber needs of the water sector. The initial establishment of the WRRO could reasonably be supported through a Congressional appropriation directly or through USEPA's budget. Long-term, the WRRO would need to select a sustainable funding approach, such as a fee system that is based on the number of customers served to equitably support the development of performance standards and compliance assessments. Keeping such costs as low as possible will be crucial to success. So, too, will be developing new mandatory performance standards that provide the greatest return on investment for cybersecurity. The analysis that follows suggests options for how America's water systems can organize a collaborative approach that effectively addresses our shared cybersecurity needs.

STRENGTHENING THE CYBER RESILIENCE OF AMERICA'S WATER SYSTEMS: INDUSTRY-LED REGULATORY OPTIONS

SECTION I: MAXIMIZING THE VALUE OF MANDATORY CYBERSECURITY STANDARDS FOR US WATER SYSTEMS

Mandatory standards for cybersecurity are not a panacea. Based on the experience of other infrastructure systems, such standards can be time-consuming to develop and may lag behind rapidly emerging threats. Voluntary measures play a critical role in enabling infrastructure system operators (including in the water sector) to meet these emerging challenges, over and above their compliance with mandatory cybersecurity requirements.

Nevertheless, mandatory standards can establish a much-needed "floor" for cyber resilience. Properly designed, mandatory standards can also give utilities considerable flexibility in deciding how to meet performance goals and other requirements. Enforcement mechanisms tailored to meet water system needs can also help ensure that across the nation, water utilities are bolstering their security in ways that the sector itself (in collaboration with USEPA) has determined are most vital.

The most effective and efficient way to develop mandatory standards is to build on the foundation established by existing guidelines. For water systems, that foundation includes the National Institute of Standards and Technology (NIST) Cybersecurity Framework ("CSF")[1] and section 2013 of America's Water Infrastructure Act of 2018 (AWIA).[2] Cybersecurity recommendations published by the USEPA and water sector associations provide a critical baseline for supporting foundation the objectives described in this paper . Notable examples:

- The American Water Works Association's *Cybersecurity Guidance & Tool,* which is sector-specific approach for implementing the NIST CSF;[3] and
- The Water Information Sharing and Analysis Center (WaterISAC) *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*.[4]

Another opportunity to help develop new security standards and a supporting organizational framework for them lies in drawing on lessons learned from other sectors. A number of sectors offer valuable models in this regard – though each of them, including the water sector, has their

[1] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[2] America's Water Infrastructure Act of 2018, pp. 86-91,https://www.congress.gov/115/bills/s3021/BILLS-115s3021enr.pdf,

[3] American Water and Wastewater Association*, Water Sector Cybersecurity Risk Management Guidance and Assessment Tool, https://www.awwa.org/cybersecurity*

[4] WaterISAC, *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*, June 3, 2019, https://www.waterisac.org/fundamentals

own unique characteristics that standards and governance mechanism need to reflect. This study leverages an especially prominent example: the Bulk Power System (BPS), which is comprised of electricity generation, transmission, and control systems.[5]

In the BPS, electric utilities and an industry organization -- the North American Electric Reliability Corporation (NERC) – work to develop standards that are vetted and then either approved or, on rare occasions, rejected by the Federal Electricity Regulatory Commission (FERC). FERC serves the federal oversight function, while NERC develops and assesses compliance with approved standards. The proven value of this approach: if the sector helps draft the standards that they know will be enforced against them, they will be supportive of the enforcement system that "holds the stick" over them to create accountability. Put a different way: because they are in on the takeoff, they are in on the landing. This approach is also structured to encourage a high degree of shared action to support systems with compliance challenges.

No equivalents to NERC or FERC exist in the water sector. This paper examines options to provide similar oversight functions to support cybersecurity risk management in the water sector. As noted in the executive summary, one option is to establish a Water Risk & Resilience Organization (WRRO) to lead the development of mandatory standards, with strong participation by water sector representatives. The WRRO would also conduct compliance audits based on the standards and hold systems accountable for any significant performance shortcomings. There may be some consideration to establish a water sector counterpart to FERC to provide federal oversight of the standards implemented by the WRRO. A faster and lower- cost alternative would be to have the USEPA lead the oversight functions given existing role for water systems, complemented by support from other federal agencies. In particular, Congress could grant authorities to the USEPA necessary for:

- Requiring the WRRO to develop minimum cybersecurity performance standards;
- Supporting the WRRO in drafting those standards with technical expertise, specialized threat information, and other types of assistance with the support of the Department of Homeland Security (DHS), the US intelligence community, and other Federal agencies;
- Improving cyber threat information and analysis;
- Reviewing and either approving or rejecting the standards proposed by the WRRO;
- Conducting enforcement-related activities, including the establishment of penalty guidelines.

[5] *Bulk-Power System* means facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof), and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. 18 CFR § 39.1 – Definitions, https://www.law.cornell.edu/cfr/text/18/39.1

Building on USEPA's existing relationship with the water sector, this co-regulatory approach offers the most expedient and least burdensome option to advance cybersecurity risk management relative to creating a new FERC-like entity for the water sector.

In one crucial respect, however, the BPS model exemplifies what *not* to do. Congress and the electric industry only moved to transition from voluntary to mandatory standards after a catastrophic blackout occurred on August 14, 2003. The massive disruptions created by that event made the need for enforceable requirements incontrovertible and politically practical.

The water sector should not wait for an equivalent catastrophe. The attack on the Oldsmar (FL) water utility operating system, and intelligence community (IC) assessments that cyber threats targeting operating systems are intensifying nationwide, verifies that a clear and present danger exists. This reality necessitates a move beyond the existing regulatory environment that includes the establishment of mandatory standards for the water sector in a narrowly focused, affordable, and sector-specific manner.

The analysis that follows is structured help the water sector and their government partners consider options to establish a co-regulatory framework. The study is organized into the following sections:

I. From Ransomware to Nation State Attacks: Aligning Standards with the Spectrum of Threats. Cyber criminals pose an immediate and growing threat to infrastructure operators. But threats to drinking water and wastewater systems also need to be placed in a broader geopolitical context. Water service is vital for US defense installations for national security more broadly. That importance makes the water sector a potential target for China, Russia, and other potential (and extraordinarily capable) adversaries, and reinforces the need to shift towards mandatory standards. AWIA provides valuable mandates for community water systems serving 3,300 or more persons to conduct risk and resilience assessments and developing emergency response plans. Now, given the intensifying threats to the water sector, system operators and their government partners should consider establishing addition requirements and – of crucial importance – determine which categories of systems would fall under them. Section I offers criteria to support that decision-making.

II. Specific Cyberattack Vectors and Implications for Standards Development. This portion of the study examines specific mandatory standards that the industry might find useful, and how they can be structured with sufficient flexibility to enable their effective and efficient implementation. While existing statutes and voluntary guidelines provide an ideal starting point to develop mandatory standards, two other factors could also prove helpful. The first, based on the model of the BPS, is to sequence the development of standards in ways that are programmatically efficient. The second is to prioritize standards that reflect recent trends in attack vectors – above all, the growing risk that adversaries will corrupt the supply chains for critical water sector hardware and software and use those compromises to conduct system-disabling attacks.

This section provides an overview of options to account for all of these potentially useful sources of input. That analysis also explores ways that standards can be structured so that they set firm requirements for cybersecurity but give the water sector latitude to determine how best to achieve those standards. Appendix A provides a more detailed analysis of specific standards that the water sector and USEPA might consider for development, based on precedents set by the BPS and the NIST CSF.

III. Structuring a Regulatory System for Mandatory Standards: Options for Governance, Standards Development, and Enforcement. The BPS regulatory framework offers a set of models that water sector operators and the USEPA might leverage. However, as briefly noted above, the water sector differs in fundamental ways from the electricity subsector, and structural options should be developed to best serve the unique needs of the water and wastewater sector. This section:

- Identifies options to organize a regulatory system the provides for mandatory, enforceable cybersecurity standards, and to allocate roles and responsibilities between industry and government;
- Examines how these participants might develop standards and (with USEPA playing a crucial role) approve them for enforcement; and
- Creates mechanisms for auditing compliance with standards and enforcing them – ideally in ways that minimize the likelihood of costly litigation.

IV. Conclusions and Possible Next Steps. The final section of the study offers summary recommendations for the water sector and USEPA to consider – above all, the need to avoid waiting for a catastrophe to strike before developing a stronger co-regulatory framework for developing and enforcing cybersecurity standards.

II. FROM RANSOMWARE TO NATION STATE ATTACKS: ALIGNING A CO-REGULATORY FRAMEWORK WITH THE SPECTRUM OF THREATS

In May 2021, the Department of Homeland Security's intelligence office issued a call to arms to the water and wastewater sector. DHS warned that "high profile cyber-attacks against water and wastewater systems (WWS) sector networks will increase as criminal, nation-state, and terrorist cyber actors seek to exploit enduring vulnerabilities to achieve financial, geopolitical, or ideological objectives."[6] The Department recommended that water sector utilities take new measures to protect their Operational Technology (OT) systems, including the Industrial Control

[6] DHS Office of Intelligence and Analysis, *Malicious Cyber Actors Likely to Continue Exploiting Vulnerabilities in Water and Wastewater Systems Networks*, May 20, 2021, http://www.orwarn.org/uploads/news/(U)%20IIF%20-%20Malicious%20Cyber%20Actors%20Likely%20to%20Continue%20Exploiting%20Vulnerabilities%2005202021.pdf

Systems (ICS) that increasingly guide water treatment operations, pumping, and other vital functions. However, the range of potential attackers identified by DHS also has broader implications for bolstering the current regulatory environment, including which categories of water systems ought to be subject to mandatory standards.

A. RANSOMWARE AND OTHER NEAR-TERM THREATS

Criminals are using infrastructure systems as their personal ATMs. To examine why the intensifying threat environment requires stronger regulatory frameworks for critical infrastructure, the starting point is to assess the types of cyberattacks that are most likely to occur. Ransomware attacks are of special concern. On June 3, 2021, the US Department of Justice warned that "recent ransomware attacks – including the attack last month on the Colonial Pipeline – underscore the growing threat that ransomware and digital extortion pose to the Nation, and the destructive and devastating consequences that ransomware attacks can have on critical infrastructure."[7]

The Biden Administration has urged the water and wastewater sector to ramp up its preparedness against such challenges. On June 2, the White House distributed a memo to sector leaders and other asset operators titled *What We Urge You To Do To Protect Against The Threat of Ransomware*. The memo stated that "To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations." Those discussions should include consensus-building on whether mandatory, enforceable mandates for restoration planning, over and above the self-reporting requirements established by the AWIA, are needed against future ransomware threats.

Water sector utilities also face threats from hackers who do not hold their systems up for ransom but nevertheless use cyber means to disrupt system operations. The February 2021 hack of the water treatment facility in Oldsmar, FL, exemplifies this threat. DHS found that unidentified cyber actors exploited unsecured remote access software to gain unauthorized access to the industrial control system (ICS) at a US drinking water treatment plant in Oldsmar, Florida. Once on the network, the unidentified cyber actors had full access to the plant's virtual human machine interface (HMI) and used that access to increase the amount of sodium hydroxide—also known as lye, a caustic chemical—in the water treatment process.[8] The hacker sought to raise the levels of sodium hydroxide being used to treat water by more than 100 times -- a hazardous level that could sicken customers and require the costly replacement of corroded pipes. An on-site human operator

[7] Deputy Attorney General Lisa Monaco, Memorandum: Guidance on Investigations and Cases Related to Ransomware and Digital Extortion, June 3, 2021, https://www.documentcloud.org/documents/20797189-signed-memorandum-ransonware-and-digital-extortion

[8] DHS, Malicious Cyber Actors

quickly restored the plant to the proper levels.[9] However, the risk of more sophisticated and successful hacks will continue to grow as new, low-cost malware becomes widely available on the darknet.[10]

Insider threats pose a further cybersecurity challenge. According to a recently unsealed Federal indictment, on March 27, 2019, a former employee of the Post Rock Rural Water District in Kansas "recklessly caused damage" to the system. In particular, he manipulated the system's controls that shut down the processes which affect the facility's cleaning and disinfecting procedures with intention to harm.[11] Guidance's from the water sector recommends voluntary measures to deal with potential insider threats. In the WaterISAC' s *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*, recommendation #4 (("Enforce User Access Controls") discusses the importance of properly disabling credentials for separated employees to minimize damage that that they could cause through unauthorized access – physical or computer."[12] Such initiatives are essential. Going forward, however, personnel security initiatives will need to encompass more severe threats than disgruntled employees – including the risk that China or other nation state adversaries will recruit utility insiders to assist cyberattack planning and execution.

B. WATER SYSTEM CONTRIBUTIONS TO NATIONAL DEFENSE AND US SECURITY

The drinking water and wastewater systems contribute to the defense of the United States in ways that are underappreciated and, in some cases, poorly understood. The most immediate contribution is that of enabling US Department of Defense installations to carry out their critical missions at home and abroad. Those bases are utterly dependent on the availability of drinking water. Defense installations also depend on drinking water service to public safety functions for fire suppression and support operational need associated with HVAC operations for computer centers, and other crucial functions. Wastewater service is just as essential for public health and safety of base operations. Indeed, absent sewerage, major defense office buildings and other national security facilities would quickly become unusable.

Adversaries are aware of these dependencies even if many Americans are not. The Department of Defense (DOD) *Mission Assurance Strategy* emphasizes the growing risk that adversaries may seek to disrupt U.S. defense capabilities indirectly, by attacking the critical infrastructure systems on which military bases depend. The Strategy warns that "The Department of Defense's ability to ensure the performance of its Mission-Essential Functions (MEFs) is at growing risk. Potential

[9] Jaclyn Peisser, "A hacker broke into a Florida town's water supply and tried to poison it with lye, police said, *Washington Post*, February 9, 2021, https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/

[10] Davey Winder, Supermarkets That Will Sell You Malware for $50," *Forbes,* April 28, 2020, https://www.forbes.com/sites/daveywinder/2020/04/28/revealed-the-supermarkets-that-will-sell-you-malware-for-50/?sh=14bed35130ae

[11] United States District Court, Kansas, *Indictment: USA versus Walter Travnicheck*, March 3, 2021, https://www.waterisac.org/system/files/articles/travnichek-indictment.pdf

[12] WaterISAC, *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*, June 3, 2019, https://www.waterisac.org/fundamentals

adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets -- within the United States and abroad -- on which our forces depend.[13]

Many current DOD initiatives to strengthen mission assurance are focused on ensuring the availability of resilient power. Those efforts are vital and should continue. However, military bases depend on drinking water and wastewater services as well. Some Defense installations have their own wells and other on-base sources of water. Many others, including the Pentagon itself, rely on a community drinking water and wastewater utility to meet their critical needs. And even if military bases have their own water sources and treatment facilities, most employees of large installations live in surrounding communities. If cyberattacks disrupt the water utility serving those employees and their families, the Defense workforces on which national security depends will be at increasing risk.

Adversaries can also jeopardize military operations by attacking the water systems that serve a broader array of defense-related assets. The *National Defense Strategy of the United States of America* notes that under DOD's Global Operating Model, the Department needs the ability to "surge" war-winning forces from their bases on US territory to conflict zones abroad.[14] Civilian-operated ports and supporting transportation systems will be essential for such surge operations. That infrastructure and the workers who operate those assets need water service – again, almost always provided by the local water system. Adversaries may target water systems accordingly. The National Defense Strategy emphasizes that "*the homeland is no longer a sanctuary*. America is a target," including for cyberattacks against private and public sector infrastructure.[15]

The importance of water sector services to national defense has significant implications for options to develop mandatory cybersecurity standards. One implication is that standards should be scaled to deal with threats from high-capability nation states. Ransomware attacks or other criminal activities will probably continue to be the most frequent type of cyber incidents that water systems face. Those attacks will also use malware that is vastly more primitive than possessed by China, Russia, and other potential adversaries. The same is true of efforts by terrorist hackers or disgruntled employees to disrupt industrial control systems in the water sector. Standards that help strengthen water sector resilience against such common (and increasingly frequent) incidents offer a prime opportunity for progress.

But we should not set the bar for cybersecurity too low. Given the vital role of the water sector in enabling DOD to prevail in future conflicts, and the corresponding risk that adversaries will target those systems for disruption, we should also consider options that can help water system operators

[13] Department of Defense, *Mission Assurance Strategy*, April 2012, p. 1, https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf
[14] Department of Defense, *The National Defense Strategy of the United States of America*, p. 7, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
[15] National Defense Strategy, p. 3 Italics in the original.

build preparedness against the most sophisticated threat vectors that nation states can employ. It may not be fair that water systems must help defend the United States from the Peoples Liberation Army's Strategic Support Force, which is responsible for conducting cyberattacks against US assets at home and abroad. But there is no escaping that harsh reality. The same is true for defense against the cyber forces possessed by Russia, North Korea, and other high-capability nations.

The Broader Value of Water to National Security – And The Broader Range Of Potential Targets

Only a relatively small number of water utilities serve military bases. The vast majority serve the residents of communities across the nation, as well as industrial, commercial, and government customers that do not directly support national defense. But these more typical water systems will not necessarily escape enemy cyberattacks. On the contrary: because they are vital to public health and safety, as well as the US economy, they may be prime targets in future international crises. This point was not lost on the former FBI Director J. Edgar Hoover, who stated in November 1941, that "It has long been recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of American populace."[16] The criticality has not changed but the threat vector has expanded with the interconnected operations of critical infrastructure systems, including water.

At present, *The National Counterintelligence Strategy of the United States of America* offers the most detailed, unclassified government assessment of why and how adversaries are targeting US infrastructure for attack. The Strategy notes that "foreign intelligence entities are developing the capacity to exploit, disrupt, or degrade critical infrastructure worldwide. Their efforts likely are aimed at influencing or coercing U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption."[17]

Attacking infrastructure essential for public health and societal well-being offers a potentially powerful means of pressuring US leaders to yield in a confrontation. The Strategy warns that "adversaries seeking to cause societal disruptions in the United States could attack the electric grid causing a large-scale power outage that affects many aspects of daily life."[18] Disrupting the water sector could cause equally drastic effects. DHS notes that "Safe drinking water is a prerequisite for protecting public health and all human activity. Properly treated wastewater is vital for

[16] John Edgar Hoover (1941), Water Supply Facilities and National Defense, *Journal – American Water Works Association, 33*(11), 1861-1865, https://doi.org/10.1002/j.1551-8833.1941.tb14956.x

[17] Office of the Director of National Intelligence, *The National Counterintelligence Strategy of the United States of America*, 2020-2022, p. 6, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf

[18] *Ibid*

preventing disease and protecting the environment. Thus, ensuring the supply of drinking water and wastewater treatment and service is essential to modern life and the Nation's economy."[19]

That assessment understates the importance of the water sector – and the disruptive effects that cyber adversaries can seek to achieve by attacking it. As with defense installations, the water sector also enables community fire suppression, dialysis centers, hospitals, as well as water flows necessary for sewerage, power generation, and other vital functions. If cyberattacks disrupt these operations, public health and the economy would face rapid and potentially catastrophic risks. The ability of the water sector to help defeat such attacks and conduct response operations to mitigate their effects are absolutely crucial for US national security.

C. MEETING THE THREAT: CURRENT STATUTORY REQUIREMENTS FOR CYBER RESILIENCE AND GAPS TO REMEDY

A strong statutory foundation already exists for drinking water and wastewater utilities and their government partners to help counter cyberattacks. The primary mission of any public water system is the protection of public health as codified in the Safe Drinking Water Act (42 U.S.C. §§ 300f – 300j–27). In similar fashion, the treatment of wastewater is to ensure public health and protect the environment from harmful pollution as codified in the Federal Water Pollution Control Act (33 U.S.C. §1251 et seq., known as the Clean Water Act (CWA). Collectively these statutes undergird the water sector's measures to provide a safe supply of drinking water, effectively manage wastewater systems, and protect public health and the environment.

The US Environmental Protection Agency supports these efforts by serving as the Sector Specific Agency and Sector Risk Management Agency for water and wastewater systems. In addition, the 2015 Water and Wastewater Sector-Specific Plan helps advance risk-based critical infrastructure protection strategies for drinking water and wastewater utilities, regulatory primacy agencies, and an array of technical assistance partners.

But these statutory foundations establish only limited cybersecurity requirements for drinking water systems. AWIA's Section 2013, *Community Water System Risk and Resilience*, is the notable exception in that it requires community water systems (CWS) serving more than 3,300 people to develop or update risk and resilience assessments and emergency response plans (ERPs). AWIA also specifies the critical assets that the risk and resilience assessments and ERPs must address and establishes deadlines by which a CWS must certify to EPA the completion of the risk and resilience assessment and ERP. These risk and resilience assessments must consider both natural hazards and "malevolent acts," and account for risks to "electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system," as well as "the monitoring practices of the system" and "the financial infrastructure of the system" (including business enterprise systems such as payroll functions, customer billing, accountants

[19] DHS, *Water and Wastewater Sector*, https://www.cisa.gov/water-and-wastewater-systems-sector

payable and banking transactions).[20] The legislation also establishes specific requirements for ERPs. These plans must include:

> (1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;
>
> (2) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;
>
> (3) actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and
>
> (4) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.[21]

These provisions establish a requirement to assess cyber risks and use those assessments to help shape emergency response plans. While AWIA establishes a mandatory duty to act, the reliance on self-assessments is limiting. CWSs subject to AWIA's requirements must certify that they have "conducted, reviewed, or revised that assessment, as applicable."[22] Neither the USEPA nor any other organization beyond the CWS submitting the certification reviews its adequacy relative to any specific cybersecurity standards or best practices. While a CWS is obligated to faithfully execute the requirements, a regulatory process that relies entirely on self-assessment and lacks any sort of external, objective auditing is inherently at risk of not being implemented consistently. Put a different way: AWIA requires drinking water utilities to act to secure their systems from cyberattacks, but those requirements are only enforceable in "after the fact" situations, where once an incident occurs, an after action review determines whether a utility adequately prepared for a cyber threat and addressed key vulnerabilities. Notably, no similar statutory requirements have been promulgated for wastewater systems under the Clean Water Act.

As water sector utilities and their partners consider options to build a stronger co-regulatory framework, consideration should also be given to the potential problems of creating unfunded mandates, and also the opportunities to help utilities receive more favorable bond ratings and insurance rates.[23]

---

[20] AWIA, p. 86
[21] AWIA, p. 88
[22] AWIA, p. 87
[23] Fitch Ratings, Cyber Events Could Pose Material Risk to Water, Sewer Utility Credit, Apr 8, 2021 https://www.fitchratings.com/research/us-public-finance/cyber-events-could-pose-material-risk-to-water-sewer-utility-credit-08-04-2021?utm_source=linkedin&utm_medium=social&utm_content=fe140c14-0c8b-4f00-a0b5-aa15b1fbda55

AWIA's section on Technical Assistance and Grants provides that the USEPA Administrator "may award grants in each of fiscal years 2020 and 2021 to owners or operators of community water systems for the purpose of increasing the resilience of such community water systems." The legislation also authorizes the Administrator to provide technical assistance to CWSs to assist in remedying system vulnerabilities "which the Administrator determines to present an immediate and urgent need."[24]

The authorized funding to actually support CWSs under these provisions would no doubt be helpful for resource constrained communities, but Congress has never appropriated the funds. Going forward, if the proposed WRRO approach is determine to be the proper course of action to establish mandatory cybersecurity standards, legislators should consider appropriating funds to help water utilities meet these cybersecurity requirements through existing programs such as the State Revolving Loan Funds (SRF), [25] the Water Infrastructure Finance and Innovation Act (WIFIA),[26] USDA Rural Assistance[27] or new funding mechanisms that Congress has deemed fit for purpose in supporting cybersecurity enhancements in critical infrastructure.

In addition, for water systems that rely on municipal or public utility commission approvals for cybersecurity spending, it would be helpful if those systems could justify their proposed spending as meeting specific, enforceable requirements. Measures taken to comply with detailed and explicit requirements could also help a utility receive more favorable bond ratings and lower their cyber insurance costs. Rating agencies and insurance underwriters are developing criteria to assess cyber threats and integrate their findings into polices for water utilities. If utilities can demonstrate that they have complied with specific cybersecurity standards, doing so will almost certainly help reduce the costs of those policies.

The AWIA provisions provide a significant advantage in setting a foundation for progress. The Act is not excessively prescriptive; it gives the water sector much-needed flexibility to adapt to evolving threats. As the water sector and USEPA consider developing mandatory standards, continuing to give utilities flexibility in how they comply with those standards will be helpful indeed. AWWA's guidance for example provides a scalable assessment that is driven by the technology applications used by the utility, versus a laundry list of prescriptive requirements that may or may not be relevant but require excessive (and low value) paperwork to validate.

To develop more detailed assessments and risk management plans, water systems can (and should) employ AWWA's *Water Sector Cybersecurity Risk Management Guidance* and analytic tool that provides a sector-specific approach for implementing the NIST Cybersecurity Framework based on their application of various technologies. [28] AWWA's resources also support the use of the

[24] AWIA, p. 89
[25] USEPA Drinking Water State Revolving Loans (SRF), https://www.epa.gov/sites/production/files/2019-10/documents/cybersecurity_fact_sheet_final.pdf
[26] USEPA, WIFIA program, https://www.epa.gov/wifia
[27] US Department of Agriculture, *Water and Environmental Programs,* https://www.rd.usda.gov/programs-services/all-programs/water-environmental-programs
[28] AWWA, *Water Sector Cybersecurity Risk Management Guidance and Assessment Tool*

Cyber Security Evaluation Tool (CSET®) developed by DHS and supported by Idaho National Lab.

The sections of this study that follow offer some specific options to bolster the standards development process, including possible measures derived from the electricity subsector that will need significant modification to meet water sector needs.

That analysis also provides options to go beyond existing mechanisms for enforcement and formal mediation of disagreements over compliance. Industries and sectors rarely jump up and down with joy when confronted with the possibility of a new regulatory enforcement mechanism. Nevertheless, given the utter dependence of US defense, national security, and public health and safety on the water sector, and the intensifying cyber threats to these systems, the time has come to consider how water systems should be subject to enforceable minimum standards through a tiered, phased approach.

D. CATEGORIES FOR APPLYING MANDATORY STANDARDS TO WATER SYSTEMS

A risk-based approach can help guide decisions on which a water utility should be covered under new cybersecurity mandates. One option is to apply specialized requirements to the systems that serve military bases designated by the Federal government as Critical Defense Facilities (CDFs). The interruption of water services to CDFs would disrupt their ability to carry out their essential missions, making the water system(s) that serve those facilities potentially attractive targets. It might be possible to adopt a risk-based approach to categorizing water systems and require CDF-supporting systems to take resilience measures over and above those applied to the rest of the sector.

Congress already requires the designation of especially critical electric systems. In the FAST ACT amendments to the Federal Power Act, legislators created two such categories. The first, "critical electric infrastructure" (CEI), includes a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters." The second category is "defense critical infrastructure" (DCEI), which includes systems that serve CDFs in the 48 contiguous States and the District of Columbia.[29] Congress might partner with the water sector, USEPA, and other agencies to develop an equivalent risk-based designation for water systems that serve critical customers.

Congress gave the Secretary of Energy specialized emergency authorities over CEI and DCEI but did not require NERC to establish additional CIP standards that would apply only to those categories of infrastructure and their operators. Future Executive Orders may require the

https://www.awwa.org/cybersecurity

[29] Federal Power Act, Section 215(a), 16 USC 824o-1: https://uscode.house.gov/view.xhtml?req=(title:16%20section:824o-1%20edition:prelim)

"responsible parties" that operate DCEI to meet specialized cybersecurity requirements. As those efforts go forward, water sector leaders may want to consider whether and how such implementation priorities and standards-setting requirements might be adapted to meet their needs.

Efforts to determine which water systems should be subject to additional standards should also account for the broader value of water service to public health and safety, and the danger that potential adversaries will target water systems to exert coercive pressure on US leaders in future crises. One possibility is to focus the application of cybersecurity requirements on water systems that serve the largest numbers of customers. For risk management formulae that focus on the potential consequences of cyberattacks, focusing on such large-scale systems would seem advantageous. These larger systems will also be more heavily dependent on sophisticated (and potentially vulnerable) industrial control systems than their smaller counterparts.

Yet, potential adversaries do not necessarily have to jeopardize public health and safety in major urban areas in order to achieve coercive leverage over US crisis decision-making. China and Russia are prepared to combine cyberattacks with information operations to magnify the public fear that even limited attacks create, and to threaten that much wider and more devastating attacks will follow unless the president yields to their demands.[30] Building preparedness against such combined attacks cannot be accomplished by applying cybersecurity standards to only those water systems that serve major urban areas. A broader reach will be essential. But how far should that applicability extend to systems that serve smaller numbers of customers?

The water sector and the partners should consider building on the categories that Congress has already established in AWIA. The Act requires all community water systems that serve 3,300 or more customers or more to comply with its mandates. Furthermore, in implementing those mandates, AWIA adopted a phased approach that gave smaller systems additional time to achieve compliance. Certifications of compliance were required significantly earlier for large systems serving a population of 100,000 than medium scale systems (serving 50,000 to 100,000) or small systems (3,300 to 50,000).[31] Equivalent categories might be established for the applicability and phased implementation of future cybersecurity standards, with water systems that serve fewer than 3,300 customers being urged to make progress on a voluntary basis to meet those standards.

III. PRIORITIES AND DESIGN PARAMETERS FOR ADDITIONAL MANDATORY STANDARDS

The structure of the water and wastewater sector is very different from that of the bulk power system. In the BPS, high voltage transmission system and other assets are tightly interconnected. Accordingly, instabilities in one utility's service area can rapidly spread to neighboring systems, unless utility operators and system components are ready to limit those instabilities and prevent

[30] Paul Stockton, *Defeating Coercive Operations in Future Crises*, Johns Hopkins University Applied Physics Laboratory, forthcoming July 2021.

[31] 42 USC 300i-2. Community Water System Risk and Resilience.

cascading failures. The infamous 1965 Northeast blackout and earlier incidents spurred transmission asset owners and operators that they needed to adopt increasingly stringent voluntary standards to reduce the danger of system-wide failures and accelerate restoration if outages occurred. The 2003 blackout convinced key elements of the electric industry, its federal agency partners, and Members of Congress that voluntary standards were no longer adequate. [32] The system of mandatory, enforceable BPS standards that exists today reflects these structural and historical forces.

The structure and evolution of the water and wastewater sector is starkly dissimilar. Many water systems function completely independent of other systems, however there are consecutive systems that are interconnected. Accordingly, when one water utility fails, there is often little or no risk that those failures will create systemic instabilities that ripple across to other regions, unless of course it is a large regional system. The historical record bears that out. The water sector has been heavily impacted by natural events like Hurricane Katrina, Superstorm Sandy, etc. but it has never had the equivalent of the 2003 blackout which was the catalyst that motivated the shift from voluntary to mandatory standards in the electric sector. Rather than wait for such a shock, the water sector and its government partners need to *anticipate* the potentially catastrophic future threats – and, ideally, avoid repeating the history experienced by the electricity subsector.

The origins of BPS standards have also shaped their content in ways that make some of them a poor fit for the water sector's needs. Many standards arose out of voluntary measures to stanch cascading failures and otherwise provide for "adequate levels of reliability" (ALR) for the bulk power system. [33] But with the rise of cyber and physical threats to the BPS, NERC has also developed mandatory Critical Infrastructure Protection (CIP) standards that more closely align with the resilience challenges confronting the water sector.

A. ADAPTING BPS STANDARDS TO MEET WATER SECTOR PRIORITIES FOR CYBER RESILIENCE

NERC was able to generate support for developing specific mandatory standards because many of those standards built on voluntary guidelines and best practices that already existed. The water sector should consider leveraging equivalent sector guidelines as the starting point for creating and expediting the development of enforceable standards. This section briefly summarizes the BPS standards that NERC currently enforces, how current water sector guidelines might help transform their content to make useful to CWS, and how standards development efforts might be sequenced in a logical and coherent way. Other infrastructure sectors have useful standards as well. This is

[32] David Nevius, *The History of the North American Electric Reliability Corporation*, https://www.nerc.com/AboutNERC/Resource%20Documents/NERCHistoryBook.pdf; Terry Boston, et al, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We* Learn? https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf

[33] NERC, *Definition of Adequate Levels of Reliability*, May 10, 2013, https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf

particularly true of the best practices developed by the Financial Services Sector and healthcare industry for supply chain risk management (SCRM).

Intensive follow-on analysis will be required to consider how each of these standards might be revamped to meet water sector needs. Appendix A provides a more detailed analysis of specific standards that the water sector and USEPA might consider for development, based on precedents set by the BPS and the NIST CSF.

"Not What, But How:" Considerations for Designing Standards

In addition to the specific NERC standards that water systems might revamp to meet their own challenges and needs, the way that NERC frames and structures these standards also offers potential best practices for the water sector to leverage. NERC seeks to develop "results-based standards" that "focus on required actions or results (the "what") and not necessarily the methods by which to accomplish those actions or results (the "how"). NERC also attempts to establish an optimal level of detail in its standards. To strike this balance, "the actions or results in a requirement should not be at too detailed of a level unless the detail is an action necessary for reliability and one for which there should be accountability. The actions or results should also not be at too high of a level; high level actions provide for accountability only when harm occurs and thus does not provide for prevention of harm occurring."

NERC also follows a "defense in depth" strategy that incorporates three types of standards:

> a) **Performance-Based** standards "define a particular reliability objective or outcome to be achieved. In its simplest form, a results-based requirement has four components: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome?"
>
> b) **Risk-Based** standards offer preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?
>
> c) **Competency-Based** standards define a minimum set of capabilities an entity needs to have to demonstrate it is able to perform its designated reliability functions. A competency-based reliability requirement should be framed as: who, under what conditions (if any), shall have what capability, to achieve what particular result or outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the bulk power system?[34]

Of course, in framing these standards, NERC's reliability focus reflects the specialized requirements of maintaining system reliability in the face of risks of cascading failures, systemic

[34] NERC, Results Based Standards, https://www.nerc.com/pa/Stand/Pages/ResultsBasedStandards.aspx

instabilities, and other risks that follow from the interconnected nature of the US grid. The risks facing US water systems are very different. Nevertheless, in considering whether and how to develop mandatory standards, the water sector should consider all three types of standards as options to meet specific cybersecurity challenges.

IV. STRUCTURING A CO-REGULATORY SYSTEM FOR MANDATORY STANDARDS: OPTIONS FOR OVERALL GOVERNANCE, STANDARDS DEVELOPMENT, AND ENFORCEMENT

The public and private sector entities that oversee the regulatory framework for BPS standards have no analog in the water and wastewater sector. Water systems, USEPA, and other stakeholders in water sector cybersecurity risk management will need to partner and create a collaborative structure that reflects the circumstances of the sector, rather than trying to mirror the electricity subsector. They will also need a process for developing and approving mandatory standards, and for auditing and enforcing their implementation by CWS.

A. GOVERNANCE

The starting point to create a governance system that oversees the development and enforcement of water sector cybersecurity standards will be an industry-led organization that can capitalize on sector expertise, coordinate initiatives, and serve as the principal point of contact for federal agencies. The most expeditious way forward may be to create a Water Risk & Resilience Organization (WRRO) to serve the industry in this fashion and perform the same basic regulatory functions of NERC.

An equally quick and effective option exists for meeting the requirements for government oversight in this co-regulatory framework. FERC, not DOE, decides whether to approve the standards developed by NERC and performs other vital functions to support BPS cybersecurity. It might be possible for Congress to require the creation of a water and wastewater sector equivalent of FERC. However, it would take many years and require significant funding to build such an organization from scratch and enable it to match FERC's cyber expertise. The recommended option is based on leveraging the existing regulatory capabilities and close industry ties possessed by USEPA, and have that agency replicate FERC's roles in the standard development process, enforcement, and other regulatory functions above and beyond those it currently performs.

B. THE STANDARDS DEVELOPMENT PROCESS

While the perception exists outside the electricity subsector that FERC usually requests NERC to develop standards, that is not the case. FERC has the authority to do so and FERC-initiated standards have proven valuable indeed. However, the majority of standards have been requested by an entity or individual, including NERC committees or subgroups and NERC staff.

A standard drafting team is typically formed with subject matter experts and together with NERC staff, the standard is drafted, balloted and sent to the NERC Board for approval. NERC utilizes a consensus-based standards development process. This development process ensures 1) those with

the technical knowledge and expertise of the complex bulk power system are engaged in the writing of the standard, 2) provides a forum where interests from all sides can develop mutually satisfactory reliability solutions and 3) balances the interest of all sizes of stakeholders. Once a standard is finalized and balloted successfully, it is presented to the NERC Board of Trustees for approval and once approved, filed with FERC and the applicable Canadian authorities. [35]

FERC's most important role is in deciding whether to approve the standards that NERC develops, regardless of which entity initiated the development process. Under the Federal Power Act (16 USC 824o(d)) the Commission is required to give due weight to the technical expertise of NERC with respect to the content of a standard. FERC must either approve the standard or reject it and (as appropriate) remand it to NERC for revision. The Commission does not have authority to dictate the specific content or text of a reliability standard, but it can approve the standard and direct NERC to develop modifications, which happens on occasion.

This model has a number of advantageous features that the water sector may want to evaluate for use by the proposed WRRO. For example, once the development of a standard begins, NERC asks BPS entities to voluntarily provide subject matter experts to do the actual drafting. That process gives NERC access to expertise beyond its own staff and helps proposed standards gain support from the utilities that help develop them. Another valuable feature: while FERC does not get to vote on internal NERC deliberations regarding the advancement of a standard towards completion and submission to the Commission, standard drafting team meetings are open to the public and FERC staffers attend to ensure they have situational awareness over development efforts. It could prove useful for the proposed WRRO to provide equivalent engagement for USEPA and other federal personnel.

C. AUDITING AND COMPLIANCE

A notable feature of the BPS regulatory system is that NERC, not FERC, has the responsibility to audit and enforce compliance with mandatory standards. NERC relies on the Regional Entities to enforce the NERC Reliability Standards with bulk power system owners, operators, and users. All bulk power system owners, operators, and users must comply with NERC-approved Reliability Standards. These entities are required to register with NERC through the appropriate Regional Entity. NERC's experience in managing these risks and maintaining its independence from those entities that comprise its members can offer water system managers valuable lessons in creating a counterpart organization.

One factor that facilitates enforcement is that because utilities and other BPS entities develop the standards that apply to them, they "know what is coming" and will already understand that they will be audited for compliance. Another factor is the expertise and perceived objectivity of NERC assessment teams in conducting audits. NERC has built that expertise over many years and has extensive training programs to keep pace with evolving standards and new technological developments. Replicating those accomplishments will take time and significant resources for the proposed WRRO.

[35] NERC, Standards Authorization Request, https://www.nerc.com/pa/Stand/Pages/SARs.aspx

Two other features of NERC's enforcement system help make it effective and relatively litigation-free. First, rather than adopt a one size fits all approach to enforcement, NERC has adopted a risk-based approach that focuses on the violations of greatest potential consequence to BPS reliability. NERC establishes Violation Risk Factors ("VRFs"), and Violation Severity Levels ("VSLs") to help guide these enforcement activities.[36] Entities are also encouraged to self-report noncompliance. Second, while most enforcement actions are settled, regional hearing processes are available to resolve contested violations or penalties or sanctions. If resolution cannot be achieved at the regional level, NERC maintains an appeal process to hear disputes. NERC not only has well-established mechanisms that enable the subjects of enforcement actions to appeal the decisions against them, but also a mediation program to resolve disputes in a more collaborative, less adversarial fashion. The program provides an informal, voluntary process in which a mediation panel helps participants to understand and work through disagreements or disputes concerning NERC performance audits.[37] Both of these features might be adapted to meet water-specific goals in developing future enforcement mechanisms.

CONCLUSION

Today's approach to cyber resilience in the water sector is a legacy of a bygone era. That approach was well-suited to the early years of the cyber era when threats to water systems were largely theoretical. They are all too real today and are becoming increasingly dangerous to US national security, the economy and community public health and safety.

A co-regulatory framework can help the water sector strengthen its cybersecurity by building on the foundations of AWIA and current sector guidelines, capitalizing on the extraordinary expertise of water sector, and relying on USEPA as the sector specific agency to support resilience efforts. The NERC-FERC structure provides a proven model of industry-government collaboration. But the water sector differs in crucial respects from the BPS, and regulatory mechanisms created for the electric system will need far-reaching modifications to be useful for water and wastewater utilities. Moreover, efforts to meet these water sector-specific needs can only succeed if the sector and USEPA lead such regulatory initiatives and closely collaborate with other stakeholders to advance cybersecurity.

Agreeing on the basic architecture of a co-regulatory framework offers a starting point for progress. An organization to represent the water sector (such as the WRRO proposed in this document) will be a critical component of the overall framework. It will be just as important to have a government partner to leverage Federal authorities and provide for reach-back to the

[36] NERC, Standard Processes Manual VERSION 4 March 1, 2019, https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

[37] NERC, Compliance and Certification Committee Hearing Procedures, Hearing Procedures for Use in Appeals, and Mediation Procedures, https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Compliance%20Certification%20Committee%20Hearing%20Procedures,%20Hearing%20Procedures%20for%20Use%20in%20Appeals,%20and%20Mediation%20Procedures.pdf

intelligence community. Rather than create a FERC-like entity from scratch, it would be more efficient and effective to build on USEPA's existing expertise and strong collaborative relationships with the water sector. Possible roles and responsibilities of these regulatory partners:

- USEPA would have the authority to require the WRRO to develop specific standards. Borrowing from the BPS model, water sector utilities and the WRRO itself might also be empowered to initiate the development of new standards.
- The WRRO would draft the cybersecurity standards, with input from USEPA and other sources of expertise, potentially including DHS and the IC.
- USEPA would either approve or reject the draft standards that the WRRO provides to it for review. If the USEPA rejects a proposed standard, it might be helpful if the Agency could remand the draft back to the WRRO with specific recommendations for revision and requirements for resubmission.
- The WRRO and USEPA would share responsibilities for compliance auditing and enforcement functions. The BPS enforcement model summarized in Appendix A illustrates one possible approach to allocating these functions. As in all other respects, however, the unique structural features and requirements of the water sector will require sector-specific solutions.

Congressional action will almost certainly be required to enable the establishment of a WRRO and grant the authorities necessary for that organization and USEPA to perform the functions summarized above. Member of Congress and their staffs are sure to have crucial insights as to how such legislation should be structured. Other sources of recommendations, including the Cyberspace Solarium Commission and the President's National Infrastructure Advisory Council, will be valuable as well. Yet, the greatest expertise on the water sector lies in the water utilities themselves. Their leadership in drafting legislative options for consideration by Congress will be essential.

APPENDIX A: HOW THE WATER SECTOR MIGHT LEVERAGE CURRENTLY ENFORCEABLE BPS STANDARDS TO HELP MEET ITS OWN, SECTOR-SPECIFIC REQUIREMENTS

The BPS standards examined below borrow from the terminology used by NERC. The water sector will almost certainly want to modify the titles of many of these standards; their overall areas of focus, however, have useful analogs for water systems. Note also that the NERC Standards employ the term "Bulk Electric System" rather than Bulk Power System. The NERC Glossary of Terms defines both terms.[38] For the purpose of this study, they will be used interchangeably. NERC also recognizes the importance of the NIST Cybersecurity Framework and works to ensure all elements of the NIST framework's voluntary efforts are taken into consideration and tracked to all mandatory CIP standards. The sections below identify some specific NIST Framework components that apply to specific cybersecurity issues.

Cyber Security: BES Cyber System Categorization (IP-002-5.1a). The purpose of this standard is to identify and categorize BES Cyber Systems and their associated BES Cyber Assets in terms of the "adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."[39] Some of these provisions parallel components of the Asset Management recommendations in the NIST CSF.

An equivalent standard could be very useful for the water sector. Water system resources available to invest in cybersecurity are limited, and potential investments will differ in the extent of the benefits they provide. The NIST Framework and more specifically AWWA cybersecurity guidance already offers prioritized criteria system components which, if they failed, would have serious consequences for system operations – and, potentially, for public health and safety. Requiring water utility operators to "rack and stack" their components in terms of low, medium, and high criticality could help guide future investments in cybersecurity. Categorizing system components in this way can also help prioritize the implementation (and enforcement) of additional cybersecurity standards.

Cyber Security: Security Management Controls (CIP-003-8) This standard requires BPS entities to "specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)."[40] Some of these challenges are addressed by the NIST provisions regarding the Business Environment.

---

[38] NERC Glossary of Terms

[39] NERC, CIP-002-5.1a — Cyber Security — BES Cyber System Categorization, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20%E2%80%94%20BES%20Cyber%20System%20Categorization&Jurisdiction=United%20States

[40] CIP-003-8 - Cyber Security — Security Management Controls, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-003-

The water sector almost certainly needs equivalent, but sector-specific, requirements to protect their cyber assets. Incidents have already occurred involving the intentional misoperation of water utility control mechanisms and the evasion of systems for securing them. Significant variation may also exist across the water sector in terms of the strength of its security systems. Establishing mandatory requirements for consistent and sustainable security management can help ensure that all CWS "level up" to performance standards that account for intensifying threats.

Cyber Security: Personnel & Training (CIP-004-6). This standard is structured to minimize the risk against compromises that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.[41]

All water systems have procedures in place to train personnel to ensure the safe operation of water treatment plants and other key facilities. However, in terms of preparedness against cyber threats, not all systems may be keeping pace with the threat. Nation states and criminals are developing increasingly effective means to conduct personalized, hard-to-detect spear phishing campaigns to access employee accounts and OT control systems. Water systems also need to examine their preparedness against insider threats, bolster employee training to detect and counter artfully designed (and carefully camouflaged) attacker efforts to access ICS from internet-connected systems. The NIST Framework and emerging best practices in the water sector might be leveraged to establish a mandatory standard to help address all of such threats.

Cyber Security: Electronic Security Perimeter(s) (CIP-005-6) and Cyber Security: Systems Security Management (CIP-007-6). Both of these standards have significant potential applicability to meet water sector needs. The purpose of the first is to "manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."[42] The second requires BPS entities "to manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).[43] NIST Framework recommendations regarding Access control and Data Security address many of these issues.

8&title=Cyber%20Security%20%E2%80%94%20Security%20Management%20Controls&Jurisdiction=United%20States

[41] NERC, CIP-004-6 — Cyber Security – Personnel & Training, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-004-6&title=Cyber%20Security%20-%20Personnel%20&%20Training&Jurisdiction=United%20States

[42] NERC, CIP-005-6 — Cyber Security – Electronic Security Perimeter(s), https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-005-6&title=Cyber%20Security%20%E2%80%94%20Electronic%20Security%20Perimeter(s)&Jurisdiction=United%20States

[43] NERC, CIP-007-6 — Cyber Security – Systems Security Management, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-007-6&title=Cyber%20Security%20-%20System%20Security%20Management&Jurisdiction=United%20States

These two standards and their implementation by BPS entities reflect many power system design features and potential vulnerabilities that are specific to the electricity subsector. Their basic purposes, however, are very much in line with emerging water system cybersecurity needs. As follow-on work goes forward to establish potential priorities for water standards development, CIP-005-6 and CIP-007-6 should be prime areas of focus.

Cyber Security: Incident Reporting and Response Planning (CIP-008-6) This standard specifies requirements for BES entities to report "Cyber Security Incidents."[44] NIST CSF components that address the Detection Process address some of these same reporting topics. As with auditing and enforcement, incident reporting constitutes what might be considered a "touchy subject" for both power companies and water systems. Reports, especially if leaked (and exaggerated) by the press, can create risks of litigation, reputational damage, drops in stock valuations for investor-owned systems, or political problems for public or municipal utilities. Technical problems can also impede incident reporting. Until recently, many OT systems lacked the logs that allow for forensics and detailed reporting for IT systems. Finally, in infrastructure sectors that have enforceable standards, violations can lead to investigations that result in fines or other enforcement actions.

Yet, the value proposition for establishing reporting requirements is long standing. In addition to this CIP standard, NERC standard EOP-004-4 requires incident reporting. If water operators remain unaware of attacks that are occurring in the sector, they will be unable to prepare against them. The unfortunate reality of today's cyber environment is that advancements in attack technologies, techniques, and procedures often outpace the efforts of infrastructure operators to anticipate and defend against them. The SolarWinds attack and recent malware operations exemplify this asymmetric situation -- and also the imperative for rapid incident warning so that other system operators can avoid becoming victims themselves.

Establishing procedures and technical capabilities to protect the confidentiality of report data (as with data from compliance audits) will be a prerequisite for moving forward. It will be equally important to reach consensus on the level of detail that reports should require. Too much, and water systems may resist the establishment and enforcement of reporting requirements. Too little, and the reports will provide little value for defending the sector. Water sector leaders should consider launching discussions on what would constitute a "happy medium" early on in the standards development process.

Cyber Security: Recovery Plans for BES Cyber Systems (CIP-009).[45] This standard exemplifies the value of building on existing water sector requirements and best practices to establish a stronger

[44] NERC, CIP-008-6 — Cyber Security — Incident Reporting and Response Planning, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-008-6&title=Cyber%20Security%20%E2%80%94%20Incident%20Reporting%20and%20Response%20Planning&Jurisdiction=United%20States

[45] NERC, CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-009-6&title=Cyber%20Security%20-%20Recovery%20Plans%20for%20BES%20Cyber%20Systems&Jurisdiction=United%20States

regulatory framework. AWIA already mandates that certain CWSs conduct risk and resilience assessments and create emergency response plans that reflect those assessments, including cyber-related vulnerabilities. Leveraging those provisions of law, water system operators might consider opportunities to strengthen the requirements for response and recovery planning. One such opportunity will be especially important for preparedness against attacks by nation state adversaries: the risk of sustained attacks that will greatly complicate system restoration.

If a crisis with the United States prompts China or other potential adversaries to conduct cyberattacks against US water systems, those attacks are unlikely to be "one and done." US opponents will continue (and perhaps intensify) those attacks until the opponents achieve their objectives. In the electricity subsector's GridEx Exercises, threat scenarios assume that attacks will occur for many weeks; participating utilities are able to exercise their emergency plans and coordination capabilities against such long-duration challenges. Perhaps in a phased process, water sector standards might require that system response plans account for the risk that restoration operations will need to go forward in the midst of ongoing cyberattacks.

Cyber Security: Configuration Change Management and Vulnerability Assessments (CIP-010-3). The purpose of this standard is to "prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems."[46] Some components of the NIST CSF's provisions on Data Security, Information Protection Process & Procedures and Security Continuous Monitoring address similar issues. Adapting this standard to meet the challenges facing water systems could be timely and useful. Across the sector, system operators are rapidly modernizing their control systems and adopting new, digitized mechanisms to reduce their costs and improve the effectiveness of their water treatment and other operations. All such changes run the risk of opening up new attack surfaces for cyber-armed opponents. Mandatory standards may be able to help water systems manage these risks.

Cyber Security: Information Protection (CIP-011-2) This standard is structured to "prevent unauthorized access to BES Cyber System Information by specifying information protection requirements" in support of protecting BES Cyber Systems.[47] NIST CSF's provisions on Data Security, Information Protection Process & Procedures and Security Continuous Monitoring are useful in this realm as well. Adversaries are seeking to steal detailed technical knowledge of US infrastructure systems and their operational characteristics to help them plan and (if necessary) execute future attacks. Artificial Intelligence (AI) is giving China and other potential adversaries

[46] NERC, CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-010-3&title=Cyber%20Security%20%E2%80%94%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments&Jurisdiction=United%20States

[47] NERC, CIP-011-2 — Cyber Security — Information Protection, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-011-2&title=Cyber%20Security%20-%20Information%20Protection&Jurisdiction=United%20States

new tools and techniques to take advantage of this sensitive information and develop system-specific playbooks to disrupt infrastructure operations.[48] Against this intensifying threat, it is becoming all the more important to establish criteria to identify water system data that must be protected, and establish requirements to make sure those protections are built and maintained.

Cyber Security: Supply Chain Risk Management (CIP-013-1).[49] The NIST Maintenance, Security Continuous Monitoring, and Analysis provides a close analogue. Water systems should consider moving the development of an equivalent standard much further up the queue. The US Counterintelligence Strategy warns that "The exploitation of key supply chains by foreign adversaries—especially when executed in concert with cyber intrusions and insider threat activities—represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure. Foreign adversaries are attempting to access our nation's key supply chains at multiple points—from concept to design, manufacture, integration, deployment, and maintenance—by inserting malware into important information technology networks and communications systems."[50]

CIP-013-1 is the first step in developing standards for SCRM that will need to continuously evolve to keep pace with emerging threats to hardware, software, and shared services such as cloud-based data storage. CWS should carefully review CIP-013-1 and more recent SCRM initiatives in the electricity subsector to assess the potential utility for water systems. However, two sectors also have SCRM processes and emerging best practices that will be valuable to consider. The first is the HSCC Health Industry Cybersecurity SCRM Guide v2.0 (HIC-SCRiM), which offers detailed and proven methods to assess and manage supply chain risks. [51] SCRM initiatives developed by the Financial Services Sector and DHS' Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force provides detail points of reference as well for the development of SCRM standards for water systems.[52]

CIP-014-2 Physical Security. This standard purpose is to identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an interconnection. While not directly applicable to standards development for cybersecurity, water sector leaders may want to review CIP-014-2 as a reference point as they continue to strengthen the physical security of their own systems.

---

[48] National Commission on Artificial Intelligence, *Final Report,* March 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

[49] NERC, CIP-013-1 – Cyber Security - Supply Chain Risk Management, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-1&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management&Jurisdiction=United%20States

[50] Counterintelligence Strategy, 7.

[51] https://healthsectorcouncil.org/hic-scrim-v2/

[52] CISA, Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, https://www.cisa.gov/ict-scrm-task-force

AUTHOR BIOGRAPHY

Dr. Paul Stockton leads Paul N. Stockton LLC, a strategic advisory firm in Santa Fe, New Mexico. He served as Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In his current capacity, Dr. Stockton helps electric utilities, trade associations, and the Electricity Subsector Coordinating Council strengthen preparedness against emerging cyber threats. He chairs the Grid Resilience for National Security subcommittee of DOE's Electricity Advisory Committee and serves on the Strategic Advisory Council of the Idaho National Laboratory and as a Senior Fellow of the Johns Hopkins University's Applied Physics Laboratory.