

FLUSHING OUT GAPS IN CRITICAL INFRASTRUCTURE: CYBERSECURITY IN WATER UTILITIES

LINDSEY WEBB*

INTRODUCTION

On October 3, 2024, American Water, the largest water utility in the United States, was hit by a cyberattack.¹ American Water provides services in fourteen states, to eighteen military installations, and to over fourteen million people.² As a result of the cyberattack, American Water had to disconnect certain systems that stopped its billing and customer portal for over a week, causing consumer concern as to the reliability of their water.³ Attacks such as this one raise concerns as to what utilities are doing to protect their operational technology (OT) and information technology (IT) systems as cyberattacks are increasing in frequency and severity across the United States.⁴ This incident also captures another issue: the cyber-safety standards set by federal and state regulators for utilities.

The Presidential Policy Directive on Critical Infrastructure Security and Resilience, published by President Barack H. Obama in 2013, advanced a national unity of effort to “strengthen and maintain secure, functioning, and resilient critical infrastructure.”⁵ This Directive identified both energy and water as critical infrastructure sectors.⁶ Critical infrastructure sectors are systems “considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”⁷ Therefore, President Obama’s 2013 Executive Order 13636 for Improving Critical Infrastructure Cybersecurity declares it is United States policy “to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a

* J.D. Candidate, 2026, Indiana University Robert H. McKinney School of Law; B.A. 2022, Texas Christian University—Fort Worth, Texas.

1. Ray Fernandez, *What We Learned from the American Water Cyber Attack: Expert Analysis*, TECHOPEDIA (Oct. 13, 2024), <https://www.techopedia.com/news/what-we-learned-from-the-american-water-cyber-attack-expert-analysis> [https://perma.cc/3UUM-J3VK].

2. David Jones, *American Water Works reconnecting systems a week after cyberattack*, CYBERSECURITY DIVE (Oct. 11, 2024), <https://www.cybersecuritydive.com/news/american-water-reconnecting-cyberattack> [https://perma.cc/T2PG-6KGM].

3. Kate Gibson, *American Water restarting systems shut down a week ago by hackers*, CBS NEWS (Oct. 11, 2024, at 10:39 ET), <https://www.cbsnews.com/news/american-water-hack-systems-restored/> [https://perma.cc/2A24-N7CV].

4. *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, EPA (June 6, 2024), <https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities> [https://perma.cc/F7J8-ED5T].

5. Presidential Policy Directive on Critical Infrastructure Security and Resilience, 1 PUB. PAPERS 106 (Feb. 12, 2013) [hereinafter PPD 21].

6. *Id.* at 114–15.

7. *Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors> [https://perma.cc/RE5N-C2F9] (last visited Sep. 8, 2025).

cyber environment that encourages efficiency.”⁸ Through the Executive Order, President Obama directed the National Institute of Standards and Technology (NIST) to develop a “Cybersecurity Framework.”⁹ Specifically, Section 7(a) of Executive Order 13636 provides that “[t]he Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible.”¹⁰ Upon development, federal agencies are required to apply the Cybersecurity Framework to manage cybersecurity risks.¹¹ The NIST Cybersecurity Framework’s broad applicability across critical infrastructure sectors, coupled with its voluntary nature, generates security and resilience gaps for general industry issues.¹²

To address the cybersecurity and resilience of the electric grid specifically, the North American Electric Reliability Corporation (NERC) created the Critical Infrastructure Protection (CIP) Reliability Standards, which are enforced by the Federal Energy Regulatory Commission (FERC) through penalties and fines under the authority of the Department of Energy.¹³ Although derived from the NIST Framework, the NERC CIP Reliability Standards cut more tailored requirements and mandate more specific compliance deliverables.¹⁴ For example, the NIST Framework says that electric utilities should have an asset inventory to help managers understand which assets are deployed to avoid service interruptions; however, the NERC CIP Reliability Standards say that electric utilities should identify critical assets (control centers, transmission stations, generators, etc.) and then identify cyber assets at those locations that could impact the ability of those critical assets to operate.¹⁵ By identifying and enforcing express cyber-hygiene baselines for the bulk electric systems in North America, FERC better addresses foreseeable and significant cyber vulnerabilities than the Cybersecurity Framework alone.

As the 2024 cyberattack on American Water makes clear, security concerns are especially relevant to the infrastructure of water utilities in the United States. Indeed, Congress, through the Safe Drinking Water Act (SDWA), has identified the presence of cyber vulnerabilities and encouraged cyber-hygiene of

8. Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

9. *Id.* at 11741.

10. *Id.*

11. *Id.*

12. See Interview with Kurt Aikman, Senior Sec. Advisor, Midcontinent Independent System Operator (Nov. 8, 2024).

13. Rahul Awati, *North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)*, TECHTARGET (Mar. 2, 2022), <https://www.techtarget.com/searchsecurity/definition/North-American-Electric-Reliability-Corporation-Critical-Infrastructure-Protection-NERC-CIP> [<https://perma.cc/BJU9-FGQK>]; *Enforcement Reliability*, FERC, <https://www.ferc.gov/enforcement-reliability> [<https://perma.cc/8ZGQ-3K8U>] (last visited Sep. 8, 2025).

14. Interview with Danielle T. Bennett, Deputy Gen. Couns., Duke Energy (Oct. 10, 2024).

15. *Id.*

community water systems.¹⁶ To do so, the SDWA requires each community water system to prepare and certify a Risk and Resilience Assessment and an Emergency Response Plan that includes “strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system.”¹⁷ If a water utility does not qualify as a community water system, the Environmental Protection Agency (EPA) will provide voluntary guidance for them to follow.¹⁸ Although community water systems are required to perform a Risk and Resilience Assessment and prepare an Emergency Response Plan, these processes are analogous to those of the NIST Framework and the voluntary guidance provided by the Cybersecurity and Infrastructure Security Agency (CISA) in both scope and detail.¹⁹ Additionally, it is a crucial time to be considering the scope of cyber-hygiene in the water-utility space, as the Office of Inspector General for the EPA has recognized: “[i]f malicious actors exploited the [identified] cybersecurity vulnerabilities, . . . they could disrupt service or cause irreparable physical damage to drinking water infrastructure.”²⁰

This Note argues that, because the current state of cybersecurity requirements for water utilities does not adequately address foreseeable and significant cyber vulnerabilities, Congress should enact the legislation proposed as H.R. 7922. The proposed legislation establishes an organization to develop risk and resilience requirements for the water sector. This Note further argues that defining cybersecurity baselines for water utilities in a risk-based approach, like the NERC-CIP Reliability Standards for the electric grid, would better enhance the security and resilience of the Nation’s critical infrastructure. Part I of this Note explains the various types of water utilities, threats to OT and IT systems, and public interest concerns when critical infrastructures are at the mercy of a cyber-incident. Part II then considers the utility governing authorities and different approaches taken across critical infrastructures in enhancing security and resilience through cyber-hygiene. Part III argues that the water utility compliance-based approach to cyber-safety remains deficient. Part IV describes how moving toward a risk-based approach and enacting H.R. 7922 would be an avenue that more effectively addresses cyber vulnerabilities.

I. WATER UTILITY TYPES AND CYBER-THREATS

By recognizing which water utilities fall under SWDA compliance-based certification and identifying sector-specific cyber-threats, H.R. 7922 foresees

16. 42 U.S.C. § 300i-2(b).

17. *Id.*

18. *Id.*

19. *Cybersecurity Assessments*, EPA (Nov. 12, 2024), <https://www.epa.gov/waterresilience/cybersecurity-assessments> [<https://perma.cc/MUV4-WWQ6>].

20. U.S. EPA, REPORT NO. 25-N-0004, MANAGEMENT IMPLICATION REPORT: CYBERSECURITY CONCERNS RELATED TO DRINKING WATER SYSTEMS 5 (2024) [hereinafter REPORT NO. 25-N-0004], https://www.epaoig.gov/sites/default/files/reports/2024-11/full_report_-_25-n-0004t_1.pdf [<https://perma.cc/HCT5-TUS8>].

and prevents significant cyber vulnerabilities that threaten reliable public drinking water. Therefore, as the current state of cybersecurity requirements for water utilities does not adequately address these sector-specific foreseeable and significant cyber vulnerabilities, Congress should enact H.R. 7922.

A. Various Types of Water Utilities

The SDWA was established by Congress to protect the quality of drinking water in the United States.²¹ The SDWA does so by requiring the EPA to promulgate national regulations for contaminants that may pose health risks and are likely to be present in public water supplies and then allowing states to exercise enforcement authority.²² The SDWA defines the term “public water system” as:

a system for the provision to the public of water for human consumption through pipes or other constructed conveyances, if such system has at least fifteen service connections or regularly serves at least twenty-five individuals. Such term includes (i) any collection, treatment, storage, and distribution facilities under control of the operator of such system and used primarily in connection with such system, and (ii) any collection or pretreatment storage facilities not under such control which are used primarily in connection with such system.²³

There are three types of public water systems. First, a community water system is “a public water system that—(A) serves at least [fifteen] service connections used by year-round residents of the area served by the system; or (B) regularly serves at least [twenty-five] year-round residents.”²⁴ Community water systems serve most Americans and include roughly 52,000 systems.²⁵ Examples include municipal water supplies, neighborhoods providing their own water, and mobile home parks.²⁶

Second, a non-transient non-community water system is “a system that is not a Community Water System and regularly serves the same twenty-five (25) or more persons at least six (6) months per year.”²⁷ There are approximately 85,000 non-transient non-community water systems in operation in the United

21. See 42 U.S.C. § 300f *et seq.*

22. ELENA HUMPHREYS, CONG. RSCH. SERV., RL31243, SAFE DRINKING WATER ACT (SDWA): A SUMMARY OF THE ACT AND ITS MAJOR REQUIREMENTS 6 (2021).

23. 42 U.S.C. § 300f.

24. *Id.*

25. *Background on Drinking Water Standards in the Safe Drinking Water Act (SDWA)*, EPA (Apr. 5, 2024), <https://www.epa.gov/sdwa/background-drinking-water-standards-safe-drinking-water-act-sdwa> [https://perma.cc/E424-GJ3Y].

26. *Are You A Public Water System?*, IND. DEP’T OF ENV’T MGMT. (June 20, 2011), https://www.in.gov/idem/files/factsheet_owq_pws_are_you_pws.pdf [https://perma.cc/2YFB-USVK].

27. *Id.*

States.²⁸ Examples include schools, factories, and churches, which provide water to the same population as a community water system but does not do so continuously over a calendar year.²⁹

The third type of public water system is a transient non-community water system. A transient non-community water system is “a system that is not a Community Water System and does not regularly serve at least twenty-five (25) of the same persons over six (6) months per year.”³⁰ There are roughly 18,000 transient non-community water systems in the United States.³¹ Examples include gas stations, grocery stores, and campgrounds where water is accessible to the public but not necessarily the same people.³²

Showing how water utilities may range in size and organization within a single state, Indiana has three main types of community water systems. First, a conservancy district utility is created when landowners, through a circuit court process, organize a not-for-profit special taxing district to provide water services within that district.³³ Valparaiso Lakes Area Conservancy District, for example, provides water, well, and sewer services to residents in the 2,623-acre watershed area north of Valparaiso.³⁴

Second, a community water system in Indiana may be an investor-owned utility, which “can be a private company where only a selection of people can invest, a publicly traded company where anyone can be a shareholder, or a subsidiary of a larger private or public company.”³⁵ For example, Indiana American Water is a publicly traded water utility company serving over one million people throughout seven Indiana counties.³⁶

Third, a community water system may be a municipal utility, which is where a city or town acquires, owns, or operates its own water utility overseen by a town council or similar legislative body.³⁷ For example, Rising Sun Municipal Utilities provides water to the City of Rising Sun’s 1,600 residential and commercial consumers.³⁸ Through these examples, it is clear there is a large range in size and organization of water utilities within Indiana. With water utilities having diverse goals, few compliance-based expectations, and no

28. EPA, *supra* note 25.

29. *Id.*

30. IND. DEP’T OF ENV’T MGMT., *supra* note 26.

31. EPA, *supra* note 25.

32. *Id.*

33. IND. CODE § 14-33 *et seq.* See also *Indiana Utility Guide*, IND. UTIL. REGUL. COMM’N 59 (2023), <https://www.in.gov/iurc/files/IURC-2023-Utility-Guide.pdf> [<https://perma.cc/G2DZ-NDPF>].

34. See VALPARAISO LAKES AREA CONSERVANCY DISTRICT, <https://vlacd.org> [<https://perma.cc/6H2M-J6X6>] (last visited Oct. 27, 2025).

35. IND. UTIL. REGUL. COMM’N, *supra* note 33, at 59.

36. *Indiana American Water*, IND. BUILDERS ASS’N, <https://buildindiana.org/member-directory/indiana-american-water/> [<https://perma.cc/Q9PF-9LZY>] (last visited Nov. 18, 2024).

37. IND. UTIL. REGUL. COMM’N, *supra* note 33, at 59.

38. *Municipal Utilities*, CITY OF RISING SUN, <https://cityofrisingsun.com/departments/municipal-utilities/> [<https://perma.cc/N9JC-VFQE>] (last visited Nov. 18, 2024).

required risk-based cyber-hygiene baselines, drinking water is increasingly vulnerable to cyber-threats.

B. Cyber-threats: Social Engineering, Outdated Technology, and Ransomware

Because of rapidly increasing cyber-threats, such as social engineering (e.g., phishing scams) and outdated technology creating opportunities for malware installation, protecting water utilities from cyber-threats demands a multi-faceted strategy merging advanced technology, employee training, and strong cybersecurity policies.³⁹ Based on the accumulation of incidents, the EPA stated that “a cyberattack on a vulnerable water system may allow an adversary to manipulate operational technology, which could cause significant adverse consequences for both the utility and drinking water consumers.”⁴⁰ The potential adverse consequences include “disrupting the treatment, distribution, and storage of water for the community, damaging pumps and valves, and altering the levels of chemicals to hazardous amounts.”⁴¹

On October 8, 2024, the Office of Inspector General for the EPA identified ninety-seven drinking water systems, serving approximately twenty-seven million people, as having critical cybersecurity vulnerabilities.⁴² That investigation accentuates the imperative to understand the types of cyber-threats that face water utilities, address potential adverse consequences, and implement strategies to encourage cyber-hygiene. As a deficiency of cyber-hygiene results in significant public safety risks, water utility cyber-hygiene initiatives must be implemented and enforced.

A cyber-threat that can be prevented by advanced technology, employee training, and strong cybersecurity policies is a social engineering campaign. Social engineering exploits vulnerabilities by tricking people into responding to phishing emails or sharing personal and professional information that helps threat-actors impersonate them.⁴³ Phishing campaigns are becoming increasingly convincing. Indeed, the “all-threats security information source” for water sectors, the Water Information Sharing and Analysis Center, has been made aware of two cyberattack attempts within six months that targeted Maine water operators with emails asking employees to click a link to “verify” information or risk having their water license revoked.⁴⁴ Addressing social engineering

39. Ankita Patel, *How to Protect Water and Wastewater Treatment Facilities from Cyber Threats?*, ON THE SPOT NEWS (Nov. 22, 2024), <https://www.otsnews.co.uk/how-to-protect-water-and-wastewater-treatment-facilities-from-cyber-threats/> [https://perma.cc/9C5Y-PFX4].

40. EPA, *supra* note 4.

41. *Id.*

42. REPORT NO. 25-N-0004, *supra* note 20, at 5.

43. Practical Law Data Privacy & Cybersecurity, Practice Note, *Cybersecurity Tech Basics: Malware and End User Attacks: Overview*, W-003-4711 (2024).

44. (TLP:CLEAR) Threat Advisory—Another Phishing Campaign Impersonates State CDC Drinking Water Program, WATERISAC (July 3, 2024, at 13:35 ET), <https://www.waterisac.org/portal/tlpclear-threat-advisory—another-phishing-campaign-impersonates-state-cdc-drinking-water> [https://perma.cc/SZX3-RMT8].

vulnerabilities through increased employee education can help prevent adverse consequences.

Additionally, operating on outdated technology leaves water utilities vulnerable to attack. Water utilities have outdated technology because facilities tend to “allocate resources to physical infrastructure in need of replacement or repair (e.g., pipes) rather than IT/OT infrastructure.”⁴⁵ As outdated technology often lacks both the processing power and memory to run the latest necessary security features to protect against modern-day malware, threat-actors can leverage such vulnerabilities and compromise critical devices or systems.⁴⁶ The common use of outdated control systems exposes industrial control systems, such as human-machine interfaces, to public wireless networks where foreign actors can use a variety of techniques to gain remote access and make changes to the underlying OT.⁴⁷ For example, threat-actors can exploit a Remote Desktop Protocol that is insecurely connected to the Internet to infect a network with ransomware, which “may lead to loss of system control, denial of service, or loss of sensitive data.”⁴⁸

Ransomware in particular is an increasing type of cyber-threat to water utilities.⁴⁹ Threat-actors leveraging social engineering or outdated technology can gain unauthorized access to a computer system, software, or electronic data and install malware designed to disable or block access until a ransom is paid.⁵⁰ For example, in 2021, a string of ransomware attacks targeted Supervisory Control and Data Acquisition servers, which required the water utilities to run their treatment systems manually until the invasions could be investigated and cleared.⁵¹ A Supervisory Control and Data Acquisition system monitors water levels, turns pumps on or off to move water through pipes, adds chemicals, and adjusts water pressure.⁵² Thus, protecting the Supervisory Control and Data Acquisition systems from threat-actors should be a prioritized cyber-hygiene practice, as altering those systems can have significant and detrimental impacts on consumers, such as stopping water distribution or adding dangerous

45. Cybersecurity Advisory, *Ongoing Cyber Threats to U.S. Water and Wastewater Systems*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Oct. 25, 2021), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a> [<https://perma.cc/6NWU-M4R6>].

46. *Id.*; see also Practical Law Data Privacy & Cybersecurity, *supra* note 43.

47. *Defending OT Operations Against Ongoing Pro-Russia Hactivist Activity*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (May 1, 2024), <https://media.defense.gov/2024/May/01/2003454817/-1/-1/0/DEFENDING-OT-OPERATIONS-AGAINST-ONGOING-PRO-RUSSIA-HACKTIVIST-ACTIVITY.PDF> [<https://perma.cc/P95R-D65Q>].

48. Cybersecurity Advisory, *supra* note 45.

49. See, e.g., *Rising Ransomware Threat To Operational Technology Assets*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY 1 (June 2021), https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf [<https://perma.cc/V373-JXSJ>].

50. Practical Law Data Privacy & Cybersecurity, *supra* note 43.

51. Cybersecurity Advisory, *supra* note 45.

52. U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-106744, *CRITICAL INFRASTRUCTURE PROTECTION: EPA URGENTLY NEEDS A STRATEGY TO ADDRESS CYBERSECURITY RISKS TO WATER AND WASTEWATER SYSTEMS* 7 (2024).

chemicals to drinking water.⁵³ By keeping technology up to date, training employees on cyber risks, and developing strong cybersecurity policies, water utilities can help prevent adverse consequences caused by ransomware. Because cyberattacks on water utilities threaten public safety and health, strong cyber-hygiene initiatives must be implemented and enforced across the water sector.

C. Public Interest Concerns

In the wake of cyber-threats, people throughout the United States face significant public health and safety concerns. Water utilities and governmental units running them also face economic strife because of the potential aggregate adverse effects of cyberattacks disrupting the reliability of water utilities. Section 1433 of the SDWA defines resilience against cyber-attacks as “the ability of a community water system or an asset of a community water system to adapt to or withstand the effects of a malevolent act . . . without interruption to the asset’s or system’s function, or if the function is interrupted, to rapidly return to a normal operating condition.”⁵⁴ When a water utility’s asset or system is interrupted, the water utility must continue to meet consumer demands through the implementation of an effective, resilient, and sector-specific Emergency Response Plan to reliably ensure safe consumer drinking water.

Reliability and resiliency are interconnected to support not only the individual customer but also the entire nation. Many water utilities strategically allocate capital infrastructure investments toward emerging technological interventions to improve the efficiency and reliability of key processes like water purification, bulk transfer, and storage processes.⁵⁵ However, the benefits of increased digitization, connectivity, and greater flexibility also introduce significant cybersecurity risks.⁵⁶

The main technological integration that increases risk is the swift convergence of IT and OT systems through the adoption of the Industrial Internet of Things (IIoT).⁵⁷ The IIoT is “a network of intelligent devices connected to form systems that monitor, collect, exchange and analyze data . . . to enhance manufacturing and industrial processes.”⁵⁸ Although IIoT predictive maintenance and asset tracking results in increased efficiency, it also increases security risks.⁵⁹ The biggest risks associated with IIoT are the commonality of

53. *See id.*

54. 42 U.S.C. § 300i-2(h).

55. George Stathos, *Water utilities: Six focus areas to help build cyber resilience*, ERNST & YOUNG (Oct. 4, 2021), https://www.ey.com/en_cn/insights/power-utilities/water-utilities-six-focus-areas-to-help-build-cyber-resilience [<https://perma.cc/WW2S-LUYX>].

56. *Id.*

57. *Id.*

58. Alexander Gillis, Brien Posey & Linda Rosencrance, *What is the industrial internet of things?*, TECHTARGET, <https://www.techtargget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT> [<https://perma.cc/HCA5-Q3EP>] (last visited Feb. 7, 2025).

59. *Id.*

IIoT devices continuing the use of default passwords; transmitting data as clear text, making it easy for a threat-actor to intercept the data; and, having other resources and devices within the connected network readily accessible, which enables threat-actors who have obtained access to launch systemic attacks through the insecure IIoT device.⁶⁰ Many water utilities have placed their devices on an IIoT, connecting OT devices, such as water pumps, to IT resources to automate and regulate their operations cost-effectively.⁶¹ When this connection is made without cybersecurity protections, threat-actors will attempt to and may succeed in logging into the water utility firewall. The city of Hale Center, Texas, encountered this risk in January 2024, when a threat-actor was able to log into the firewall, and water overflowed into the city.⁶² Because cyberattacks impact how drinking water utilities function, the EPA says that water system managers need to “know when their treatment systems, pumps, valves, tanks, etc. are being compromised, how to stop an attack, and how to recover so that safe and full service can be returned to the community.”⁶³ By recognizing the nexus between reliability and resilience, water utilities can identify the developing risks and implement protocols to ensure public health and safety concerns, and economic strife, do not result from cyberattacks.

Because safe drinking water is imperative for public health and safety, proper cyber-hygiene should be implemented to increase water utility resiliency. Water utilities of all sizes are vulnerable targets for threat-actors because if reliability falters, there is a potential to “disrupt civilian infrastructure and cause widespread panic.”⁶⁴ Over ninety-two percent of the nation supplied by community water systems consistently receive drinking water that meets all health-based standards, but threat-actors have the potential to alter the levels of chemicals to hazardous amounts.⁶⁵ For example, on February 5, 2021, threat-actors obtained unauthorized access to the Supervisory Control and Data Acquisition system of a water treatment facility in the city of Oldsmar and increased the levels of sodium hydroxide in the water.⁶⁶ If the water treatment

60. *Id.*

61. Jessica Balen, *Public Utilities Benefit from the Industrial Internet of Things But Must Secure It*, STATE TECH (Oct. 9, 2024), <https://statetechmagazine.com/article/2024/10/public-utilities-benefit-from-iiot-security-perfcon> [https://perma.cc/V333-GMHL].

62. *Id.*

63. *Drinking Water Infrastructure Resilience and Sustainability Research*, EPA (Nov. 8, 2024), <https://www.epa.gov/water-research/drinking-water-infrastructure-resilience-and-sustainability-research> [https://perma.cc/VG2K-3GDV].

64. Jonathan Reed, *Cyberattack on American Water: A warning to critical infrastructure*, SECURITY INTELLIGENCE (Nov. 4, 2024), <https://securityintelligence.com/news/cyberattack-on-american-water-warning-critical-infrastructure/#:~:text=Attackers%2C%20particularly%20nation%2Dstate%20actors,systems%20are%20easier%20to%20breach> [https://perma.cc/NN3Q-KB67].

65. *Safe Drinking Water Act (SDWA)*, EPA (Oct. 6, 2025), <https://www.epa.gov/sdwa> [https://perma.cc/Q8U6-5NVF].

66. Cybersecurity Advisory, *Compromise of U.S. Water Treatment Facility*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 12, 2021), <https://www.cisa.gov/news-events/>

personnel had not been able to identify and mitigate this cyberattack when they did, the 15,000 people drinking the Oldsmar City water would have been severely sickened.⁶⁷

In addition to the health concerns, there are nationwide public interest concerns with the potential for economic strife that can result from cyberattacks on such a critical infrastructure. The Value of Water Campaign's economic impact analysis found that on a national level, "a one-day disruption in water service represents an aggregate daily loss of \$43.5 billion in sales and \$22.5 billion in GDP. For context, an eight-day national disruption in water service would amount to a one percent loss in annual GDP—putting roughly 1.9 million jobs at risk."⁶⁸ To prevent a disruption in water services, water utilities must do all that they can to mitigate cyber vulnerabilities through cyber-hygiene. The costs for larger water utilities can be millions to recover data and fix infected systems. For smaller water utilities, because they do not have the same number of resources or personnel to help with recovery, the costs of a cyberattack can cripple their operations. But ultimately, the costs of a cyberattack will be borne by the consumer in their water rate prices. Therefore, the potential adverse aggregate effects of an unreliable water utility, as a result of cyber-threats, are felt in both public health and safety concerns and economic strife. To ensure reliability and mitigate cyber vulnerabilities, water utilities should not only understand what the standard of cyber-hygiene is but also how those standards are governed and enforced.

II. HOW WATER UTILITIES ARE APPROACHING CYBERSECURITY

By understanding the broad federal agency guidance for cyber-hygiene and comparing the EPA compliance-based approach to cybersecurity for water utilities with the risk-based approach of the NERC CIP Reliability Standards for the electrical grid, it becomes clear that EPA's "checking a box" approach is not ideal for addressing foreseeable cyber-vulnerabilities within such a critical infrastructure. Therefore, because the current compliance-based cybersecurity requirements for water utilities do not adequately address these significant vulnerabilities, Congress should enact H.R. 7922, which would create sector-specific risk-based approaches to water utility cybersecurity.

cybersecurity-advisories/aa21-042a [https://perma.cc/H8ZV-JKXL]; Frances Robles & Nicole Perlroth, *'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town*, N.Y. TIMES (Feb. 8, 2021), <https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html> [https://perma.cc/J4AX-AMKU].

67. Robles & Perlroth, *supra* note 66.

68. *New Analysis Finds Closing the Investment Gap in Water Infrastructure Would Create 1.3 Million Jobs, \$220 Billion in Economic Activity*, U.S. WATER ALL. (Mar. 22, 2017), <https://uswateralliance.org/new-analysis-finds-closing-the-investment-gap-in-water-infrastructure-would-create-1-3-million-jobs-220-billion-in-economic-activity/> [https://perma.cc/UC2T-78QH].

A. A Patchwork of Federal Agency Guidance

The Presidential Policy Directive on Critical Infrastructure and Resilience intentionally provided a broad approach to cybersecurity to be applicable across all sectors through its identification of sixteen critical infrastructure sectors.⁶⁹ The Directive created room for sector-specific engagement and support but failed to delegate an adequate standard for agencies to create specific guidance or implementation standards.⁷⁰ As a result, there is a patchwork of federal guidance aimed at improving cyber-hygiene across critical infrastructures, which falls short of sector-specific needs when implemented without a specific sector in mind. The most notable support agencies are NIST, as it pioneered cybersecurity guidance in critical infrastructures; CISA, as it developed additional performance goals and serves as a resource for reporting cyberattacks; and the Federal Bureau of Investigation (FBI), as it leads the investigation process for cyberattacks against critical infrastructures.⁷¹

Although NIST provides cybersecurity standards, guidelines, and best practices to prioritize and address cybersecurity risks, it does not specify actions for meeting those outcomes.⁷² The NIST Framework, created from the direction of Executive Order 13636, maintains its “level of detail and specificity . . . [so that it remains] scala[ble] and flexib[le]” for a wide range of organizations.⁷³ As this flexibility allows for the NIST Framework to be adopted in all sixteen critical infrastructure sectors, the “one-size-fits-all” approach cannot sufficiently address cybersecurity concerns in sector-specific circumstances. Therefore, the NIST Framework leaves significant gaps in cyber safety for critical infrastructures that do not adopt additional cyber-hygiene methods. For example, NIST’s Quick Start Guide for analyzing gaps and creating an action plan asks entities to “establish, test, deploy, and maintain hardened baselines that enforce the organization’s cybersecurity policies and provide only essential capabilities.”⁷⁴ By presenting procedural instructions without a scaffolding of concrete criteria, the guidance creates loose compliance standards that cause resource-constrained critical infrastructures, such as municipal water utilities, to be disadvantaged.

With the NIST Framework as a jumping-off point, CISA collaborates with state and local partners as well as other agencies to defend against cyber-threats

69. PPD 21, *supra* note 5, at 114–15.

70. *See id.*

71. *See id.*

72. *Frequently Asked Questions*, NAT’L INST. OF STANDARDS & TECH. (Sep. 24, 2024), <https://www.nist.gov/cyberframework/faqs> [<https://perma.cc/CE96-3A9M>].

73. NAT’L INST. OF STANDARDS & TECH., INITIAL SUMMARY ANALYSIS OF RESPONSES TO THE REQUEST FOR INFORMATION (RFI): EVALUATING AND IMPROVING CYBERSECURITY RESOURCES: THE CYBERSECURITY FRAMEWORK AND CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT 5 (2022).

74. NAT’L INST. OF STANDARDS & TECH., NIST CYBERSECURITY FRAMEWORK 2.0: QUICK-START GUIDE FOR CREATING AND USING ORGANIZATIONAL PROFILES (2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1301.pdf> [<https://perma.cc/K65B-HRK8>].

with the goal of creating a secure and resilient infrastructure.⁷⁵ CISA created the voluntary Cross-Sector Cybersecurity Performance Goals that align with the NIST Framework and set recommended actions such as having “[a]t least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security.”⁷⁶ However, the Cross-Sector Cybersecurity Performance Goals are not comprehensive and do not identify all the cybersecurity practices needed to protect national and economic security and public health and safety.⁷⁷ Beyond this guidance, critical infrastructure owners and operators are required to report covered cybersecurity incidences and ransomware payments to CISA under the Cyber Incident Reporting for Critical Infrastructure Act of 2022.⁷⁸ CISA then coordinates response and investigation efforts with the state and local government as well as relevant agencies such as the FBI.

The FBI collects and shares intelligence with critical infrastructures that have suffered a cyber incident and serves as the lead federal agency for investigating cyberattacks.⁷⁹ Investigating cyber-incidences is paramount for building a resilient future because it identifies the scope of the invasion, deters threat-actors from launching additional attacks, and helps industries learn which cybersecurity strategies are inadequate. Of the ransomware attacks reported to the FBI in 2023, almost half of them targeted critical infrastructure sectors.⁸⁰ As water utilities are targeted due to their vitality to public health and national economic security, understanding sector-specific authorities and approaches is important for the identification of cybersecurity gaps.

B. Water Utility Authorities and Approaches for Cybersecurity

As the Presidential Policy Directive on Critical Infrastructure and Resilience designates the EPA as the lead agency for water sector security, the

75. *About CISA*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/about#:~:text=Security%20and%20Resilience.-,CISA's%20Work,inrastructure%20security%2C%20and%20emergency%20communications> [https://perma.cc/55M6-MGRP] (last visited Nov. 26, 2024).

76. *Cybersecurity Performance Goals (CPGs)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/cybersecurity-performance-goals-cpgs> [https://perma.cc/2MMG-UF2L] (last visited Nov. 26, 2024).

77. *Id.*

78. 6 U.S.C. § 681(b); Practical Law Data Privacy & Cybersecurity, Practice Note, *Critical Infrastructure Cybersecurity and Cyber Incident Reporting: Overview (US)*, W-043-8602 (2024).

79. *The Cyber Threat*, FBI, <https://www.fbi.gov/investigate/cyber#:~:text=The%20FBI%20is%20the%20lead,cyber%20activities%2C%20wherever%20they%20are> [https://perma.cc/D4C6-LBXE] (last visited Nov. 26, 2024).

80. Matt Kapko, *Ransomware attacks are hitting critical infrastructure more often, FBI says*, CYBERSECURITYDIVE (Mar. 11, 2024), <https://www.cybersecuritydive.com/news/ransomware-hitting-critical-infrastructure-fbi/709814/#:~:text=More%20than%202%20in%205,1%2C193%20hit%20critical%20infrastructure%20organizations> [https://perma.cc/5W2B-EVPJ].

EPA provides technical, outreach, and education assistance to state, local, and private water systems to develop their own cyber-hygiene standards.⁸¹ When a community water system serves fewer than 3,300 people, the EPA encourages it to refer to a linked guidance and assessment tool to gauge the utility's cybersecurity practices, focusing on identifying, protecting, detecting, responding, and recovering.⁸² When a community water system serves more than 3,300 people, the EPA requires it to certify to a Risk and Resiliency Assessment and an Emergency Response Plan every five years; however, the EPA does not require specific standards, methods, or tools to fulfill any certain requirements.⁸³ Therefore, comparing the identified goals to the reality of compliance-based cybersecurity implementation and enforcement generates visibility into sector-specific cyber vulnerabilities for water utilities.

To certify to the EPA, a utility must only acknowledge six components in its Risk and Resiliency Assessment:

1. the risk to the system from malevolent acts and natural hazards;
2. the resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;
3. the monitoring practices of the system;
4. the financial infrastructure of the system;
5. the use, storage, or handling of various chemicals by the system; and
6. the operation and maintenance of the system.⁸⁴

The EPA provides a Vulnerability Self-Assessment Tool (VSAT) that can be downloaded in an app and filled out using multiple-choice and short-answer responses to assist a utility in assessing those six components.⁸⁵ In that tool, the utilities answer questions about the demographics of their utility service area, any mutual aid or assistance agreements between other utilities in circumstances when a rapid response is needed, and any minimum daily treatments performed during periods of non-functionality in order for the EPA to gather pertinent data

81. *Water and Wastewater Systems Sector Cybersecurity*, EPA (June 23, 2024), <https://www.epa.gov/climate-change-water-sector/water-and-wastewater-systems-sector-cybersecurity> [<https://perma.cc/9FJY-XZ8W>].

82. *Cybersecurity Assessments*, *supra* note 19.

83. *AWIA Section 2013/SDWA Section 1433: Risk and Resilience Assessments and Emergency Response Plans*, EPA (Aug. 14, 2024), <https://www.epa.gov/waterresilience/awia-section-2013#RRA> [<https://perma.cc/E32A-BL6X>].

84. *Id.*

85. *See VSAT Web Data Entry Guide*, EPA, <https://vsat.epa.gov/vsat/> [<https://perma.cc/FH8V-XVNG>] (last visited Nov. 24, 2025).

and to identify risks.⁸⁶ After a water utility submits its Risk and Resiliency Assessment, it must prepare an Emergency Response Plan that incorporates the Risk and Resiliency findings.⁸⁷ In the Emergency Response Plan, each utility must include individual strategies and procedures that focus on resilience and detection.⁸⁸ Although each utility has flexibility in developing its plan, the EPA provides a Community Water System Emergency Response Plan Template that outlines factors that need to be included in any response plan, such as an emergency internal and external communication strategy, and links to mitigation action guides such as the CISA Cyber Hygiene Scanning and Testing Services.⁸⁹

During the latest five-year certification period, approximately ninety-eight percent of community water systems serving more than 3,300 people certified to the EPA that they had completed a Risk and Resiliency Assessment and an Emergency Response Plan, as required by the SDWA Section 1433.⁹⁰ However, since September of 2023, over seventy percent of the systems inspected by the EPA were “in violation of basic SDWA Section 1433 requirements including missing specific sections of the RRA and ERP.”⁹¹ Examples of alarming cybersecurity vulnerabilities that EPA inspectors identified included failing to change default passwords, using single logins for all staff, neglecting to rescind access to former employees, and not including an assessment of resilience.⁹²

The EPA exercises its enforcement discretion on a case-by-case basis for community water systems that do not comply with SDWA Section 1433 requirements.⁹³ The enforcement discretion includes the authority to seek a civil penalty of up to \$69,733 each day in which such violation occurs or commence a civil action to require a water utility to comply.⁹⁴ However, the EPA has only taken a little over one hundred SDWA enforcement actions since 2020 for community water systems that do not comply with SDWA Section 1433 requirements despite over seventy percent of reporting community water

86. *Id.*

87. EPA, *supra* note 83.

88. *Id.*

89. EPA Off. of Water, *Community Water System Emergency Response Plan Template*, EPA (Sep. 2024), <https://www.epa.gov/system/files/documents/2024-10/community-water-system-emergency-response-plan-template-and-instructions.pdf> [https://perma.cc/HQ5D-SVS3].

90. *Get Ready for Round 2 of AWIA Section 2013 RRA and ERP Requirements*, AM. WATER WORKS ASS'N VIRGINIA SECTION, <https://vaawwa.org/stories/get-ready-for-round-2-of-awia-section-2013-rra-and-erp-requirements> [https://perma.cc/4QC4-XLRL] (last visited Nov. 27, 2024).

91. EPA, *supra* note 4.

92. *Id.*

93. EPA, AMERICA'S WATER INFRASTRUCTURE ACT SECTION 2013/ SAFE DRINKING WATER ACT SECTION 1433 FAQs 7 (2024), https://www.epa.gov/system/files/documents/2023-10/awia_s2013_faqs.pdf [https://perma.cc/D569-2MSG].

94. *Id.*

systems being in violation.⁹⁵ Therefore, the reality of cyber-hygiene for water utilities, under the current EPA strategy of collecting certifications of Risk and Resiliency Assessments and Emergency Response Plans, appears to be an inadequate way of addressing and correcting real cybersecurity risks for the critical infrastructure of drinking water as cyberattacks on the sector are increasing in frequency.

C. Electric Utility Authorities and Approaches for Cybersecurity

The Federal Powers Act requires an Electric Reliability Organization to develop mandatory reliability standards, which become enforceable after FERC review and approval.⁹⁶ FERC appointed NERC as the Electric Reliability Organization.⁹⁷ FERC then approved NERC's first eight CIP Reliability Standards, which requires users, owners, and operators of the Bulk-Power System to comply with specific requirements aimed at safeguarding critical cyber assets.⁹⁸ The NERC CIP Reliability Standards provide a comprehensive risk-based methodological set of requirements and clear penalties with the goal of promoting industry behavior that supports reliability.⁹⁹ That framework demonstrates how sector-specific regulatory oversight can effectively drive cybersecurity improvements across critical infrastructure. Water utilities face similar OT and IT security challenges and could benefit from an analogous regulatory structure that accounts for the unique characteristics of community water systems. A water sector-specific framework, similar to the NERC CIP Reliability Standards, could establish clear cybersecurity expectations, enforcement mechanisms, and penalties while considering the cyber risk realities in different types of water utility facilities.

The NERC CIP Reliability Standards, with the weight of law, require that electric utilities follow specific standards to “identify critical assets, create control mechanisms, enforce the logical and physical security of their systems, and recover any affected assets following a cybersecurity incident.”¹⁰⁰ One strategy the NERC CIP Reliability Standards uses is to compare the immediate difference between the actual power being exchanged and the power scheduled

95. EPA, *supra* note 4; Cf. EPA, REPORT NO. 23-P-0003, THE EPA MET 2018 WATER SECURITY REQUIREMENTS BUT NEEDS TO IMPROVE OVERSIGHT TO SUPPORT WATER SYSTEM COMPLIANCE 11 (2022), https://www.epa.gov/system/files/documents/2023-02/_epa_oig_20221208-23-P-0003_REPORT.pdf [<https://perma.cc/LMQ5-4SH8>] (“Approximately [nineteen] percent of water systems did not certify that they had completed their risk and resilience assessments . . . These noncompliant water systems may not be aware of their vulnerability to malevolent acts that could result in loss of service or unsafe drinking water. Furthermore, [ninety-five] percent of the noncompliant water systems were small water systems.”).

96. 16 U.S.C. § 824o; Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368, 7369 (Feb. 7, 2008) (codified at 18 C.F.R. pt. 40).

97. Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368.

98. *Id.*

99. *Id.*

100. Awati, *supra* note 13.

to be exchanged, with adjustments for factors like frequency bias, meter errors, and automatic time error correction to measure how reliably a power system can supply the demand placed on it.¹⁰¹ The NERC CIP Reliability Standards then specify the accuracy and availability requirements in a Violation Severity Level chart measuring from low to severe.¹⁰² A Violation Severity Level “defines the degree to which compliance with a requirement was [or was not] achieved.”¹⁰³ A Violation Risk Factor considers requirements that “if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.”¹⁰⁴ By comparing the Violation Severity Levels to Violation Risk Factors, an electric utility can gauge what is expected of them for different NERC CIP Reliability Standards and what fines can be expected for different degrees of violations.¹⁰⁵

FERC exercises its enforcement discretion by having Regional Entities (Midwest Reliability Organization, Northeast Power Coordinating Council, ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, and Western Electricity Coordinating Council) monitor NERC CIP Reliability Standards compliance using tools like audits, spot checks, and investigations of the electric utilities within their regional boundaries.¹⁰⁶ Those Regional Entities then administer penalties pursuant to the Violation Severity Levels and Violation Risk Factors.¹⁰⁷ The administrated penalties assure mitigation of future violations and ensure that the sanctions bear a reasonable relation to the seriousness of the violation and factors such as the utility’s ability to pay, concealment, and multiple violations.¹⁰⁸

These NERC CIP Reliability Standards violation penalties range from one thousand dollars to one million dollars per violation per day.¹⁰⁹ NERC does not take this responsibility lightly, as there were 970 reported noncompliance

101. See N. AM. ELEC. RELIABILITY CORP., RELIABILITY STANDARDS FOR THE BULK ELECTRIC SYSTEMS OF NORTH AMERICA (2024), <https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCCompleteSet.pdf> [<https://perma.cc/W94S-LNSR>].

102. See *id.*

103. See N. AM. ELEC. RELIABILITY CORP., VIOLATION RISK FACTOR AND VIOLATION SEVERITY LEVEL JUSTIFICATIONS (2016), https://www.nerc.com/pa/stand/project%20201602%20modifications%20to%20cip%20standards%20dl/2016-02_cip_vrf_and_vsl_justification_clean_10212016.pdf [<https://perma.cc/SW76-QVMC>].

104. *Id.*

105. See *id.*

106. See *Compliance & Enforcement*, N. AM. ELEC. RELIABILITY CORP., <https://www.nerc.com/pa/comp/Pages/Default.aspx> [<https://perma.cc/82D4-G5ZM>] (last visited Nov. 25, 2025).

107. *Id.*

108. N. AM. ELEC. RELIABILITY CORP., SANCTION GUIDELINES OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION 1 (2014), https://www.nerc.com/pa/Stand/Resources/Documents/Appendix_4B_of_the_Rules_of_Procedure_Sanction_Guidelines.pdf [<https://perma.cc/C6LV-X6C7>].

109. *Id.* at 14.

incidences investigated in 2023.¹¹⁰ Of those reported, only 120 were determined to be moderate to severe risk violations.¹¹¹ As the investigation process and penalties for noncompliance are robust, ninety percent of utilities correct the immediate issue that led to the noncompliance and implement steps to minimize future recurrence within one year of a noncompliance reporting date.¹¹² Therefore, the reality of cyber-hygiene for electric utilities, under the current risk-based NERC CIP Resiliency Standards, is an effective way of addressing and correcting real cybersecurity risks for the critical infrastructure of electricity.

III. A DEFINED RISK-BASED CYBERSECURITY BASELINE FOR WATER UTILITIES IS NEEDED

As the current compliance-based approach to water utility cyber-security has neither shown to prevent threat-actors from taking advantage of system vulnerabilities nor been enforceable against all vulnerable water utilities, the current approach is inadequate. In comparison, the risk-based approach to electric utility cyber-security provides baselines and enforceable standards to allow electric utilities to develop cyber-hygiene in a flexible and industry-specific manner. Therefore, because current cybersecurity requirements for water utilities cannot adequately address foreseeable and significant cyber vulnerabilities in a compliance-based approach, Congress should enact H.R. 7922, which would create a means for a sector-specific risk-based approach to cybersecurity.

A. Water Utility Cybersecurity Remains a Deficiency

Because of underreaching baselines and a lack of resources, the current compliance-based approach to cyber-hygiene does not adequately address foreseeable and significant cyber vulnerabilities for water utilities as emphasized in the number of cyberattacks.¹¹³ Due to the number of systems and the range of community water system sizes, cybersecurity challenges faced by drinking water utilities may differ from other critical infrastructure sectors that have fewer providers.¹¹⁴ Therefore, having only compliance-based cyber-hygiene initiatives, such as certification to a self-performed and self-developed Risk and Resiliency Assessment and an Emergency Response Plan every five

110. N. AM. ELEC. RELIABILITY CORP., ORGANIZATION REGISTRATION AND CERTIFICATION PROGRAM AND COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM ANNUAL REPORT 17 (2024), <https://www.nerc.com/pa/comp/CE/ReportsDL/2023%20CMEP%20and%20ORCP%20Annual%20Report.pdf> [<https://perma.cc/33XD-R7FV>].

111. *Id.* at 18.

112. *Id.* at 22.

113. *See* EPA, *supra* note 4.

114. ELENA HUMPHREYS, CONG. RSCH. SERV., IN12311, SAFE DRINKING WATER ACT (SDWA) CYBERSECURITY PROVISIONS 1 (Jan. 29, 2024).

years with standards analogous to the broad NIST Framework and CISA guidance, is inadequate. The compliance-based protocols currently in place for water utilities create a perilous regulatory landscape that inadvertently provides threat-actors with opportunities to exploit cyber vulnerabilities and adversely impact the nation by making drinking water unreliable.

A key issue with the current EPA cyber standards is underreaching baselines. The SDWA requires the EPA to “provide baseline information on malevolent acts of relevance to community water systems.”¹¹⁵ Black’s Law Dictionary defines a baseline as “the starting point for comparison.”¹¹⁶ However, the EPA only notes a general risk of cyberattacks and references flexible resources such as CISA’s Top Cyber Actions for Securing Water Systems and NIST’s Guide to OT Security.¹¹⁷ Conservancy district water utilities, investor-owned water utilities, and municipal water utilities range in sophistication and scale of their OT systems and are all vulnerable to cyberattacks; therefore, understanding the risks of cyberattacks coupled with general guidance is a starting point but not a solution.¹¹⁸

In the Top Cyber Actions for Securing Water Systems resource, CISA provides an outline of mitigating actions with links to free services and resources.¹¹⁹ The overview consists of reducing exposure to the public-facing Internet, conducting regular cybersecurity assessments, changing default passwords immediately, and reducing exposure to vulnerabilities.¹²⁰ In the Guide to OT Security resource, NIST provides an overview of OT, general threats, and specific recommendations for each type of threat.¹²¹ For example, the Guide to OT Security mentions when remote maintenance capabilities exist, an organization is advised to consider whether multi-factor authentication is productive for protecting OT environments due to it being an accepted best practice for remote access to OT applications.¹²² Therefore, although the voluntary flexible resources provide information about malevolent acts of relevance to community water systems, the starting point for cyber vulnerability risk and mitigation comparison is not clear because there are no well-defined sector-specific performance measurements of risk-based standards. This is demonstrated by CISA’s shallow Top Cyber Actions for Securing Water

115. 42 U.S.C. § 300i-2(a).

116. *Baseline*, BLACK’S LAW DICTIONARY (2d ed. 2024).

117. *See Baseline Information on Malevolent Acts for Community Water Systems Version 3.0*, EPA 24 (May 2024), https://www.epa.gov/system/files/documents/2024-05/baseline_information_malevolent_acts_508_050724.pdf [<https://perma.cc/2THQ-34SM>].

118. *See* IND. UTIL. REGUL. COMM’N, *supra* note 33, at 59.

119. *Top Cyber Actions for Securing Water Systems*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 23, 2024), <https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf> [<https://perma.cc/2HUE-W5U2>].

120. *Id.*

121. *See* KEITH STOUFFER ET AL., NAT’L INST. OF STANDARDS & TECH., GUIDE TO OPERATIONAL TECHNOLOGY (OT) SECURITY (2023), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf> [<https://perma.cc/VBN6-4QBA>].

122. *Id.* at 41.

Systems and NIST's cross-sector Guide to OT Security.¹²³ The issue of underreaching baselines is conveyed in the frequency of cyberattacks.¹²⁴

In addition to the national-level reporting requirements exempting almost eighty percent of water systems from reporting, state, local, and municipal governments are not included as covered entities.¹²⁵ Many community water systems are municipal utilities; Indiana alone has 392 municipal water utilities.¹²⁶ Exempting vulnerable systems from reporting cyber incidents creates an incomplete picture where the actual number of cyberattacks likely exceeds what is publicly known and reported. The EPA Water Infrastructure and Cyber Resilience Division provided the “[c]onservative estimate of threat likelihood” to be, on average, at least one attempted cyberattack annually on every water system.¹²⁷ The likelihood of future cyberattack attempts is exacerbated by a lack of resources.¹²⁸

Because drinking water utilities range in operation size, they also range in the amount of staff and budgeting resources available.¹²⁹ It is often the case for smaller water utilities not to have dedicated threat intelligence or cyber hunting teams, as they have a finite amount of personnel already “wearing multiple hats.”¹³⁰ For example, the City of Elkhart provides over three billion gallons of drinking water to consumers but has only fifteen full-time operators.¹³¹ Even larger operations such as Aqua Indiana, having three public water systems serving 100,000 people, have a Security Operations Team, yet it only has forty-five employees working within Indiana.¹³² Therefore, simply providing voluntary guidance that requires the water utility to develop its own technical assessments and emergency plans adds potentially unachievable goals to the already stressed workforce. In connection to the lack of resources, many small utilities falling out of the SDWA Risk and Resiliency and Emergency Response Plan certification requirements assume they will not be targets of a

123. See EPA, *supra* note 4.

124. *Id.*

125. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 52, at 23.

126. *Municipal Utilities—A Brief Regulatory Overview*, IND. OFF. OF UTIL. CONSUMER COUNS. (July 2020), <https://www.in.gov/oucc/watersewer/tips-and-publications/municipal-utilities-a-brief-regulatory-overview/#:~:text=487%20water%2C%20electric%20and%20natural,and%20town%20governments%20in%20Indiana> [<https://perma.cc/X6P8-PDQ9>].

127. EPA, *supra* note 117, at 24.

128. Aikman, *supra* note 12.

129. See IND. UTIL. REGUL. COMM'N, *supra* note 33, at 58–59.

130. Aikman, *supra* note 12.

131. *2024 Water and Wastewater Utility Annual Presentation to the City Council*, CITY OF ELKHART (2024), <https://elkhartindiana.org/wp-content/uploads/2024-Presentation-for-FY23.pdf> [<https://perma.cc/6YNJ-L67X>].

132. *Aqua Indiana*, AQUA AM. (2025), <https://www.aquawater.com/about-aqua/states-serve/aqua-indiana> [<https://perma.cc/3TTF-4XG7>].

cyberattack.¹³³ However, ninety-five percent of public water systems in the nation are considered small under the SDWA, serving 10,000 or fewer people, and an aggregate attack against them could be especially devastating.¹³⁴

Those smaller utilities represent a significant vulnerability to our national water infrastructure because they lack adequate cybersecurity protections despite being attractive targets for threat-actors. On April 19, 2024, the Tipton West Wastewater Treatment Plant in Indiana was the target of a cyberattack.¹³⁵ Tipton Municipal Utilities provides water and wastewater treatment for a town of 5,000 people residing about forty miles north of Indiana's capital.¹³⁶ Although those affected were shocked to learn that a foreign actor was targeting their little town, their cybersecurity scare was not an anomaly, as "recent cyberattacks by groups affiliated with Russia and Iran have targeted smaller communities."¹³⁷ Therefore, having only compliance-based cyber-hygiene initiatives creates a voluntary regulatory landscape that inadvertently provides threat-actors with opportunities to exploit underreaching baselines and a lack of resources. The cyber vulnerabilities throughout drinking water utilities adversely impact the nation by making drinking water less reliable.

*B. NERC CIP Reliability Standards are a Successful
Example of Cyber-Hygiene*

Because NERC CIP Reliability Standards adequately address sector-specific cyber vulnerabilities with clear risk-based baselines and enforceable standards, the current bulk electric system risk-based approach to cyber-hygiene adequately addresses foreseeable and significant cyber vulnerabilities for electric utilities. The NERC CIP Reliability Standards serve the important goal of electric reliability while remaining reasonable, nondiscriminatory, non-preferential, and in the public interest.¹³⁸ Therefore, by having risk-based cyber-hygiene standards with accompanying mitigation guidance and penalties, NERC CIP Reliability Standards build upon the NIST Framework and CISA

133. See Rich Nye, *Russian hackers take responsibility for cybersecurity attack on Tipton wastewater treatment plant*, 13 WTHR (Apr. 25, 2024, at 9:23 EDT), <https://www.wthr.com/article/news/local/russian-hackers-claim-responsibility-for-cybersecurity-attack-on-tipton-indiana-wastewater-treatment-plant/> [<https://perma.cc/V49X-CB6T>].

134. *21st Annual EPA Drinking Water Workshop: Small System Challenges and Solutions*, EPA (Nov. 8, 2024), <https://www.epa.gov/water-research/21st-annual-epa-drinking-water-workshop-small-system-challenges-and-solutions> [<https://perma.cc/5XPR-DZV9>].

135. Nye, *supra* note 133.

136. Anna Ribeiro, *Hackers target Tipton Municipal Utilities wastewater treatment plant, prompting federal investigation*, INDUS. CYBER (Apr. 23, 2024), <https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-tipton-municipal-utilities-wastewater-treatment-plant-prompting-federal-investigation/> [<https://perma.cc/6PSQ-N9E2>].

137. *Cyberattacks on water systems are increasing, EPA warns, urging utilities to take immediate action*, CBS NEWS (May 20, 2024, at 18:46 EDT), <https://www.cbsnews.com/news/cyberattacks-on-water-systems-epa-utilities-take-action/> [<https://perma.cc/8KGE-NAN7>].

138. Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368.

guidance to create a regulatory landscape that intentionally considers threat-actors with opportunities to exploit cyber vulnerabilities in electric utilities.¹³⁹

NERC CIP Reliability Standards provide clear risk-based baselines without imposing only one way to accomplish compliance.¹⁴⁰ FERC approved of NERC CIP Reliability Standards having measurable baselines and examples of ways to be compliant with the risk-based standards as well as delegating the creation of guidance to the Electric Reliability Organization to allow utilities “to implement measures adapted to their specific situations more consistently and effectively.”¹⁴¹ Advantages of risk-based compliance include enhanced resilience, the ability to adapt to evolving threats, and customized security measures.¹⁴² Accordingly, the baselines recognize that not all utilities connected to the bulk electric system have identical risks, but having risk-based cyber-hygiene standards with accompanying mitigation guidance and penalties allows FERC to adequately address foreseeable and significant cyber vulnerabilities for electric utilities.

One of the keyways that electric utility risk-based compliance is reasonable is that the Electric Reliability Organization updates known industry risks as they develop.¹⁴³ FERC and NERC gauge whether the industry, or segments of the industry, are having difficulty implementing standards and what cyber-hygiene standards effectively prevent attempted cyberattacks from being successful cyberattacks through “more frequent, semi-annual, self-certifications.”¹⁴⁴ NERC CIP Reliability Standards requires each utility to provide an impact rating signed by an executive in the company updated every fifteen months.¹⁴⁵ Additionally, the Regional Entities perform an annual audit to provide information and statistics to FERC about each NERC CIP Reliability Standard and how the electric utilities in each Regional Entity identify risk and compliance.¹⁴⁶ Most entities connected to the bulk electric system truly view the NERC CIP Reliability Standards as a baseline and implement additional more robust practices.¹⁴⁷ Therefore, the risk-based baselines and enforceable standards allow electric utilities to develop cyber-hygiene in a flexible and industry-specific manner.

139. Interview with Danielle T. Bennett, *supra* note 14.

140. Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368.

141. *Id.*

142. *Enhancing Grid Security: The Role of Risk-Based Compliance in NERC CIP*, NETWORK PERCEPTION (Oct. 25, 2023), <https://www.network-perception.com/blog/enhancing-grid-security-the-role-of-risk-based-compliance-in-nerc-cip#:~:text=This%20approach%20involves%20assessing%20and,consequences%20of%20a%20security%20breach> [https://perma.cc/97T9-KKEB].

143. *See* Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368, 7369.

144. *Id.*

145. Interview with Danielle T. Bennett, *supra* note 14.

146. N. AM. ELEC. RELIABILITY CORP., *supra* note 109.

147. Aikman, *supra* note 12.

A. Enactment of H.R. 7922

Because the current compliance-based cybersecurity requirements for water utilities do not adequately address foreseeable and significant cyber vulnerabilities, the EPA should move to a risk-based approach, like the NERC-CIP Reliability Standards, which would better enhance the reliability and resilience of drinking water. Although most industries, water sector inclusive, do not want the government to come in and set up rules and regulations, there is no evidence that the water sector is acting in a meaningful way of its own volition here, and the movement from compliance-based voluntary guidelines to risk-based required standards requires legislation to give the EPA enforcement authority.¹⁴⁸ On April 10, 2024, “Congressmen Rick Crawford (AR-01) and John Duarte (CA-13) introduced H.R. 7922, the Water Risk and Resilience Organization (WRRO) Establishment Act . . . [to establish] a new governing body, the WRRO, with cyber and water-system expertise to develop and enforce cybersecurity requirements for drinking water systems.”¹⁴⁹

H.R. 7922 proposes that the WRRO develop water-sector-specific standards and then monitor the implementation and compliance.¹⁵⁰ The WRRO will utilize “advanced technical knowledge and expertise in the operations of covered water systems” to develop and implement cybersecurity risk and resilience measurement requirements, in line with prevailing best practices, that “provide for an adequate level of cybersecurity risk and resilience” for community water systems.¹⁵¹ As for monitoring, the WRRO will annually submit an aggregated data findings report on the implementation and effectiveness of cybersecurity risk and resilience requirements to the EPA.¹⁵² They will then have the authority to impose penalties of up to \$25,000 per day if the utility is in violation.¹⁵³

H.R. 7922 is inspired by the success of NERC in developing, implementing, and enforcing the NERC CIP Reliability Standards.¹⁵⁴ NERC has successfully established sector-specific cybersecurity baselines that enhance bulk electric system resilience through flexible, risk-based approaches, allowing the critical infrastructure to adapt security measures to their operational environments while maintaining accountability through executive-signed impact ratings.¹⁵⁵ The

148. Interview with Jim Watson, Investigations, Cybersecurity & Data Priv. Couns., Ice Miller LLP (Oct. 28, 2024).

149. Sara Robertson, *Reps. Crawford and Duarte Introduce Legislation to Protect Water Systems from Cyber Threats*, U.S. CONGRESSMAN RICK CRAWFORD (Apr. 11, 2024), <https://crawford.house.gov/posts/rep-crawford-and-duarte-introduce-legislation-to-protect-water-systems-from-cyber-threats> [<https://perma.cc/BE24-2B7B>].

150. H.R. 7922, 118th Cong. (2024).

151. *Id.* § 1(c)(2)(A)–(C).

152. *Id.* § 1(e)(2).

153. *Id.* § 1(f)(4).

154. Gov’t Affs. Off., *Establishing the Water Risk and Resilience Organization*, AM. WATER WORKS ASS’N 1 (Apr. 11, 2024), <https://www.awwa.org/wp-content/uploads/WRRO-Summary-240410-164552-1.pdf> [<https://perma.cc/KXY7-ZLKB>].

155. Interview with Danielle T. Bennett, *supra* note 14.

NERC CIP Reliability Standards have merged regulatory compliance with practical security by building upon the NIST Framework and CISA guidance to create a preemptive cyber-hygiene landscape that addresses evolving threats and encourages utilities to implement practices beyond the minimum requirements.¹⁵⁶ Such a landscape aligns with the public interest for resilient and reliable utilities.

Allowing external review of cybersecurity risk and resilience to be a voluntary action is inadequate to ensure a critical infrastructure system is prepared to address cyber vulnerabilities. Therefore, the current EPA approach, of compliance equating to certification, alone needs to be addressed in legislation like H.R. 7922.¹⁵⁷ By transitioning to a sector-specific risk-based set of standards, water utilities will be able to incorporate cyber-hygiene using updated guidance based on the developments of known industry risks in a way that fits the resource capacity and risk of the individual water utility.

CONCLUSION

The Presidential Policy Directive on Critical Infrastructure and Resilience identified both energy and water as critical infrastructure sectors requiring cybersecurity measures against potential threat-actors.¹⁵⁸ In response to these identified vulnerabilities, federal regulatory bodies adopted divergent approaches: the EPA developed high-level compliance-based guidelines for drinking water utilities, whereas FERC implemented measurable risk-based standards for electric utilities connected to the bulk electric system. A comparison of the two regulatory approaches in addressing cyber vulnerabilities in critical infrastructures reveals substantial deficiencies in the cyber-hygiene protocols currently governing water utilities.

This Note argued that the current cybersecurity requirements for water utilities fail to adequately address foreseeable and significant cyber vulnerabilities, necessitating congressional action through H.R. 7922. This conclusion is supported by public interest concerns in the wake of emerging cyber-threats, the increasing amount of cyberattack attempts on water utilities, and the lack of enforcement authority for cyber standards. Furthermore, this Note argued that a comparison between the water utility compliance-based approach to cyber-safety and the electric utility risk-based approach to cyber-safety reveals a pronounced security deficiency within the water sector. FERC's risk-based methodology, with its emphasis on measurable outcomes and enforcement mechanisms, provides a more robust framework for addressing cyber vulnerabilities in critical infrastructure. To remedy these regulatory shortcomings, the EPA should transition from its current compliance-based

156. *Id.*

157. See Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368.

158. PPD 21, *supra* note 5, at 114–15.

approach to a risk-based method for cybersecurity standards with a defined measurement of compliance and meaningful enforceable authority. Implementation of this regulatory reform would be substantially facilitated by congressional enactment of H.R. 7922, which would provide the necessary statutory foundation for a more rigorous cybersecurity framework in the water sector.