Research memo

FDD | CCTI Center on Cyber and Technology Innovation

Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure

By RADM (Ret.) Mark Montgomery and Trevor Logan

November 18, 2021

Executive Summary

America's critical infrastructure is only as strong as its weakest link, and in the United States, water infrastructure may be the greatest vulnerability. The significant cybersecurity deficiencies observed in the drinking water and wastewater sectors result in part from structural challenges. The United States has approximately 52,000 drinking water and 16,000 wastewater systems, most of which service small- to medium-sized communities of less than 50,000 residents.[1] These systems operate with limited budgets and even more limited cybersecurity personnel and expertise. Conducting effective federal oversight of, and providing sufficient federal assistance to, such a distributed network of utilities is inherently difficult.

Compounding this challenge, the increasing automation of the water sector has opened it up to malicious cyber activity that could disrupt or manipulate services. This past February, a hacker nearly succeeded in raising the concentration of a caustic agent in the drinking water of a small Florida city one hundred-fold after breaching the system the utility uses for remote-access monitoring and troubleshooting. The automation of such systems reduces personnel costs and facilitates regulatory compliance, but few utilities have invested the savings from automation into the cybersecurity of their new systems.

The expanded attack surface resulting from automation could also allow hackers to cause disruptive and cascading effects across multiple critical infrastructures. "Water is used in all phases of energy production and electricity generation," the Department of Energy noted in a report on the nexus between the water and energy sectors.[2] Water and power systems are often physically interconnected.[3]

The federal government — in particular, the Environmental Protection Agency (EPA), which is the sector risk management agency (SRMA) responsible for the water sector — bears responsibility for the fragility of the sector's cybersecurity posture. The EPA is not resourced or organized to assess and support the water sector consistent with the scope and scale of the critical infrastructure challenges the sector faces. As part of its congressional mandate to

1. U.S. Department of Homeland Security and Environmental Protection Agency, "2015 Water and Wastewater Sector Specific Plan," June 2015. (https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf)
2. U.S. Department of Energy, "The Water-Energy Nexus: Challenges and Opportunities," June 2014. Page 1. (https://www.energy.gov/sites/prod/files/2014/07/f17/Water%20Energy%20Nexus%20Full%20Report%20July%202014.pdf)
3. Ibid., page 7.

assess and recommend improvements to national cyber resilience, the Cyberspace Solarium Commission (CSC) reviewed the responsibilities and performance of all SRMAs. Regarding the water sector, the CSC concluded that there is "insufficient coordination between the EPA and other stakeholders in water utilities' security."[4] The Government Accountability Office has expressed similar concerns.[5]

Water infrastructure is critical to national security, economic stability, and public health and safety. Building on the CSC's concerns regarding the vulnerability of the water sector, this paper analyzes the specific challenges facing this sector and identifies steps that utilities and the federal government — both the legislative and executive branches — should take to mitigate this national vulnerability. A layered approach combining a strengthening of the EPA, improved government financial support and oversight, and a stronger partnership between government and utilities will result in a more secure, reliable, and resilient water sector.

Specific recommendations include:

- resourcing and empowering the EPA to succeed as the water sector's SRMA and as the government lead for cybersecurity in the sector;
- directing some of the EPA's water sector grant programs exclusively toward cybersecurity issues;
- increasing funding for the U.S. Department of Agriculture's rural cybersecurity programs;
- directing the Cybersecurity and Infrastructure Security Agency to increase support for the water sector;
- increasing the federal government's financial support for water sector associations;
- encouraging water utilities to increase investments in cybersecurity technology and personnel;
- improving water utilities' access to cybersecurity training and assessment resources;
- establishing a joint industry-government cybersecurity oversight program; and
- amending the American Water Infrastructure Act to increase the cybersecurity effectiveness of water utility risk assessments.

Acronyms

AWIA – America's Water Infrastructure Act of 2018

AWWA – American Water Works Association

CISA – Cybersecurity and Infrastructure Security Agency

CSC – Cyberspace Solarium Commission

ERPs – Emergency Response Plans

FERC – Federal Electricity Regulatory Commission

IT – Information Technology

NERC – North American Electric Reliability Corporation

NIST – National Institute of Standards and Technology

NRWA – National Rural Water Association

4. U.S. Cyberspace Solarium Commission, *Final Report*, March 2020, page 62. (https://www.fdd.org/analysis/2020/03/11/cyberspace-solarium-commission-report)

5. Gene Dodaro, U.S. Government Accountability Office, "Priority Open Recommendations: Environmental Protection Agency," *Letter to Environmental Protection Agency Administrator Michael S. Regan*, June 29, 2021, page 14. (https://www.gao.gov/assets/gao-21-557pr.pdf)

OT – Operational Technology

RCAP – Rural Community Assistance Program

RRAs – Risk and Resilience Assessments

SCADA - Supervisory Control and Data Acquisition

SLTT – State, Local, Tribal, and Territorial

SRF – State Revolving Fund

SRMA – Sector Risk Management Agency

SSA – Sector Specific Agency

WaterISAC – Water Information Sharing and Analysis Center

WRRO – Water Risk & Resilience Organization

WSCC – Water Sector Coordinating Council

Increasing Threats and Stagnant Security Budgets

Across the nation, cyberattacks are increasing in both frequency and severity,[6] and the water sector is not immune.[7] In February 2021, the City of Oldsmar, Florida, suffered an attack that could have significantly compromised public health. A hacker breached the network of the city's drinking water treatment facility and manipulated the levels of chemicals used in the water purification process, attempting to increase the concentration of sodium hydroxide from its normal 100 parts-per-million (ppm) to 11,100 ppm. Sodium hydroxide, also known as lye or caustic soda, is used to manage pH in water but at elevated levels can be highly corrosive and can sicken consumers.[8]

Oldsmar city officials reassured the public that an employee witnessed the hacker's movements in real time and stopped the chemicals from being released into the water supply.[9] The officials also noted that it would have taken 24 to 36 hours for the chemicals to contaminate the water supply for the city's 15,000 residents, and system alarms would have sounded well before then.[10] The officials acknowledged, however, that the employee who witnessed the intrusion initially failed to report it, assuming it was another employee remotely accessing the network through an older program, rather than a hacker. The FBI cited poor cybersecurity, including weak passwords and outdated operating systems, as contributors to the hacker's success.[11]

6. U.S. Federal Bureau of Investigation, Internet Crime Complaint Center, "Internet Crime Report: 2020," 2020. (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

7. U.S. Cybersecurity Infrastructure Security Agency, Press Release, "Ongoing Cyber Threats to U.S. Water and Wastewater Systems Sector," October 14, 2021, (https://us-cert.cisa.gov/ncas/current-activity/2021/10/14/ongoing-cyber-threats-us-water-and-wastewater-systems-sector)

8. Gus Serino and Ben Miller, "Recommendations Following the Oldsmar Water Treatment Facility Cyber Attack," *Dragos*, February 8, 2021. (https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack); "Oldsmar's Cyber Attack Raises the Alarm for the Water Industry," *Government Technology*, February 25, 2021. (https://www.govtech.com/sponsored/oldsmars-cyber-attack-raises-the-alarm-for-the-water-industry.html)

9. Frances Robles and Nicole Perlroth, "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," *The New York Times*, February 8, 2021. (https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html)

10. Pinellas Sheriff, "Treatment Plant Intrusion Press Conference," *YouTube*, February 8, 2021. (https://www.youtube.com/watch?v=MkXDSOgLQ6M)

11. U.S. Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Environmental Protection Agency, and Multi-State Information Sharing and Analysis Center, Advisory, "Compromise of U.S. Water Treatment Facility," February 11, 2021. (https://us-cert.cisa.gov/sites/default/files/publications/AA21-042A_Joint%20Cybersecurity%20Advisory_Compromise%20of%20U.S.%20Water%20Treatment%20Facility.pdf)

Two years earlier, in March 2019, a similar attack succeeded in shutting down the treatment and disinfectant procedures at a drinking water plant in Ellsworth, Kansas.[12] The Department of Justice accused a disgruntled former employee of intentionally threatening public health and safety.[13] Despite having resigned from the company two months earlier, the employee used his still-active remote-access credentials to tamper with the system.[14]

The water sector is also under threat from state-backed hackers. In 2018, the Cybersecurity and Infrastructure Security Agency (CISA) and its interagency partners issued a joint technical alert notifying critical infrastructure stakeholders of a two-year cyber campaign by Russian intelligence to target U.S. government entities as well as non-governmental organizations in the nuclear, electricity, and water sectors.[15] In July 2020, CISA and the National Security Agency (NSA) urged owners and operators to "take immediate actions to secure" their "Internet-accessible Operational Technology (OT) assets" in light of attempted and successful attacks on critical infrastructure.[16] While the advisory did not specify the targets, it cited an attempted Iranian attack on Israel's water systems in May 2020, implying that water utilities should pay attention to this latest information.[17]

More recently, CISA, the EPA, the FBI, and the NSA issued a joint advisory and infographic warning of ongoing threats to water and wastewater systems.[18] The advisory warned that water systems are at risk because utilities are "inconsistently resourced," rely on "unsupported or outdated operating systems and software," and use "outdated control system devices or firmware versions" with known and exploitable vulnerabilities.[19] The advisory highlighted three instances in which attackers successfully deployed ransomware within a water utility's Supervisory Control and Data Acquisition (SCADA) system, forcing the facilities to switch to manual operation. Ransomware is most commonly deployed against information technology (IT) and business operations systems, but ransomware can

12. Jonathan Shorman and Steve Vockrodt, "Ex-employee tampered with Kansas water plant, feds say, a sign of online vulnerability," *The Kansas City Star*, April 11, 2021. (https://www.msn.com/en-us/news/us/ex-employee-tampered-with-kansas-water-plant-feds-say-a-sign-of-online-vulnerability/ar-BB1fwSVS)

13. Indictment, *United States v. Travnicheck*, No. 21-40029-HLT (D. Kan. filed March 31, 2021). (https://www.ksn.com/wp-content/uploads/sites/13/2021/03/travnichek-indictment.pdf); U.S. Department of Justice, U.S. Attorney's Office for the District of Kansas, Press Release, "Indictment: Kansas Man Indicted for Tampering With a Public Water System," March 31, 2021. (https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system)

14. U.S. Cybersecurity and Infrastructure Security Agency, Alert (AA21 – 287A), "Ongoing Cyber Threats to U.S. Water and Wastewater Systems," October 14, 2021. (https://us-cert.cisa.gov/ncas/alerts/aa21-287a)

15. U.S. Cybersecurity and Infrastructure Security Agency, Alert (TA18-074A), "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," March 15, 2018. (https://us-cert.cisa.gov/ncas/alerts/TA18-074A)

16. U.S. National Security Agency and Cybersecurity and Infrastructure Security Agency, Advisory, "NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operation Technologies and Control Systems," July 23, 2020. (https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF)

17. Maggie Miller, "Federal agencies warn foreign hackers are targeting critical infrastructure," *The Hill*, July 23, 2020. (https://thehill.com/policy/cybersecurity/508748-federal-agencies-warn-foreign-hackers-are-targeting-critical)

18. U.S. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency, Alert (AA21 – 287A), "Ongoing Cyber Threats to U.S. Water and Wastewater Systems," October 14, 2021. (https://us-cert.cisa.gov/ncas/alerts/aa21-287a); U.S. Cybersecurity and Infrastructure Security Agency, "Cyber Risks & Resources for the Water and Wastewater Systems Sector," October 2021. (https://www.cisa.gov/sites/default/files/publications/infographic-supply-water-national-critical-function-102021-508.pdf)

19. U.S. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency, Alert (AA21 – 287A), "Ongoing Cyber Threats to U.S. Water and Wastewater Systems," October 14, 2021. (https://us-cert.cisa.gov/ncas/alerts/aa21-287a)

also "infect connected OT systems, particularly if there is not adequate segmentation between IT and OT systems," CISA warned in an infographic released alongside the advisory.[20]

The U.S. government provides a variety of alerts and advisories to the general public as well as to specific industries. Some of these alerts describe the vectors that attackers use to target victim networks, and provide indicators of compromise to help cyber defenders understand the types of suspicious network activity they should look for. However, these technical advisories are useful only if recipients have sufficient training, tools, and resources to incorporate this threat information into existing defense efforts.

Highly publicized attacks on the water sector, along with numerous government alerts, have failed to spur a consistent implementation of cybersecurity best practices across the sector. While operation and maintenance costs for production, treatment, distribution, and collection in the sector have risen steadily over the past 60 years, federal investment in drinking water and wastewater facilities has not kept up, often forcing state and local governments (which own and operate more than 80 percent of water utilities[21]) to foot growing bills.[22] Over the past two decades, federal investment in water systems has equaled only 4 percent of the amount that state and local governments invested, and most of the federal funding was in the form of low-interest loans, not grants.[23]

Like many industries, the water sector has turned to automation to combat growing operational costs.[24] Today, water levels can be monitored remotely. Pumps and valves can be operated remotely. Even chemical treatment systems can be turned on and monitored remotely. This reliance on SCADA systems, industrial control systems, and programmable logic controllers has dramatically reduced manpower costs.[25] However, these advances have also introduced significant cybersecurity risks, as these systems are increasingly intertwined with systems connected to the internet. With the increase in high-profile attacks, the utilities that shifted to high levels of automation should have ramped up cybersecurity. They have not. Instead, many water utilities still use outdated and unpatched technologies and lack cybersecurity personnel.[26]

20. U.S. Cybersecurity and Infrastructure Security Agency, "Cyber Risks & Resources for the Water and Wastewater Systems Sector," October 2021. (https://www.cisa.gov/sites/default/files/publications/infographic-supply-water-national-critical-function-102021-508.pdf)

21. Mark Straus, "Setting The Record Straight On Investor-Owned Water Utilities," *Water Online*, June 6, 2016. (https://www.wateronline.com/doc/setting-the-record-straight-on-investor-owned-water-utilities-0001). For comparison, federal and public entities own only 16 percent of the electricity subsector. U.S. Energy Information Agency, "Electricity explained: Electricity generation, capacity, and sales in the United States," March 18, 2021. (https://www.eia.gov/energyexplained/electricity/electricity-in-the-us-generation-capacity-and-sales.php)

22. U.S. Government Accounting Office, "Private Water Utilities: Actions Needed to Enhance Ownership Data," March 2021. (https://www.gao.gov/assets/gao-21-291.pdf)

23. U.S. Congressional Budget Office, "Public Spending on Transportation and Water Infrastructure, 1956 to 2017," October 2018, page 23. (https://www.cbo.gov/system/files/2018-10/54539-Infrastructure.pdf)

24. Chris Nolan and Annie Fixler, "The Economic Costs of Cyber Risk," *Foundation for Defense of Democracies*, June 28, 2021. (https://www.fdd.org/analysis/2021/06/28/the-economic-costs-of-cyber-risk)

25. Gustaf Olsson, "Urban water supply automation: today and tomorrow," *Journal of Water Supply: Research and Technology-Aqua*, June 1, 2021, Volume 70, Issue 4, pages 420–437. (https://iwaponline.com/aqua/article/70/4/420/78365/Urban-water-supply-automation-today-and-tomorrow)

26. Jim Magil, "U.S. Water Supply System Being Targeted By Cybercriminals," *Forbes*, July 25, 2021. (https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals); William Steel, "Cybersecurity for Water Utilities," *Water World*, October 1, 2018. (https://www.waterworld.com/water-utility-management/article/16190093/cybersecurity-for-water-utilities)

Part of the problem stems from the overall budgetary challenges the water industry faces. With miles of pipelines, unpredictable variables such as droughts and severe weather, and the variance in topography and production capacity within each state, the water sector is unable to determine standardized annual water and wastewater price increases in the same commoditized way that the U.S. Department of Energy (DOE) does for the electricity subsector.[27] This has resulted in systemic underinvestment in all areas, culminating in a significant shortfall: The EPA assesses that U.S. drinking water infrastructure needs $472 billion in investment.[28] Industry association estimates are even more alarming, placing the investment need at "more than $1 trillion nationwide over the next 25 years."[29] It is difficult to invest in cybersecurity when many "utilities are struggling to maintain and replace infrastructure, maintain revenues while addressing issues of affordability, and comply with safe and clean water regulations," noted the Water Sector Coordinating Council (WSCC),[30] a sector-organized body that interacts with the EPA on the sector's behalf.[31]

The Water Industry Recognizes Its Shortcomings

Earlier this year, the WSCC and the Water Information Sharing and Analysis Center (WaterISAC)[32] surveyed over 600 drinking water and wastewater organizations to assess the sector's cybersecurity posture and challenges.[33] Survey respondents ranged in size from organizations serving fewer than 500 people to those serving more than 250,000. While the respondents varied in their ownership structures and functions within the sector,[34] consistent themes emerged — especially an uneven understanding of the threat, and underinvestment in cybersecurity programs.[35]

Sixty percent of companies surveyed spent less than 5 percent of their budget on IT security in 2021, while nearly two-thirds spent less than 5 percent on OT security. A plurality spent less than 1 percent on IT or OT security (see Figures 1 and 2).[36] Moreover, the smaller the utility, the less it spent on cybersecurity as a percentage of its budget. More than 60 percent of the smallest water utilities (those servicing fewer than 3,330 people) spent less than 1 percent on IT or OT security. These utilities often face "economic disadvantages typical of rural and urban communities. Others do not have access to a cybersecurity workforce," the report observes.[37]

27. U.S. Department of Energy, "Water and Wastewater Annual Price Escalation Rates for Selected Cities Across the United States," September 2017. (https://www.energy.gov/sites/prod/files/2017/10/f38/water_wastewater_escalation_rate_study.pdf)
28. U.S. Environmental Protection Agency, "Drinking Water Infrastructure Needs Survey and Assessment: Sixth Report to Congress," March 2018. (https://www.epa.gov/dwsrf/epas-6th-drinking-water-infrastructure-needs-survey-and-assessment)
29. "Buried No Longer," *American Water Works Association*, March 2013. (https://www.awwa.org/Portals/0/AWWA/Government/BuriedNoLonger.pdf?ver=2013-03-29-125906-653).
30. "Water and Wastewater Systems Cybersecurity 2021 State of the Sector," *Water Sector Coordinating Council*, June 2021, page 3. (https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf)
31. U.S. Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sector Partnerships: Sector Coordinating Councils," accessed September 27, 2021. (https://www.cisa.gov/sector-coordinating-councils)
32. Established in 2002 in coordination with the EPA, the Water Information Sharing and Analysis Center is the designated information sharing and operations arm of the Water Sector Coordinating Council.
33. The Cyberspace Solarium Commission and the Foundation for Defense of Democracies provided the WSCC with insights on questions that would be informative in developing a better understanding of cybersecurity challenges in the sector.
34. Surveyed organizations are members of national water and wastewater associations, including the Association of Metropolitan Water Agencies, American Water Works Association, National Association of Clean Water Agencies, National Association of Water Companies, National Rural Water Association, WaterISAC, Water Research Foundation, and Water Environment Federation.
35. "Water and Wastewater Systems Cybersecurity 2021 State of the Sector," *Water Sector Coordinating Council*, June 2021. (https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf)
36. Ibid.
37. Ibid., page 3.

Figure 1: Water Utilities Spend a Small Percentage of Their Budget on IT Cybersecurity

Percentage of 2021 Budget Allocated for IT Cybersecurity	Number of Individuals Served							
	≤500	501–3,300	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	>250,000	Total
<1%	64	54	33	33	13	11	14	222
1%–5%	6	19	18	26	20	12	29	130
6%–10%	1	0	4	10	4	6	12	37
>10%	1	3	4	4	0	3	9	24
N/A; IT cybersecurity is managed at the municipal/county government level	6	3	5	11	7	3	4	39
Do not know	17	15	20	23	14	17	28	134
Total	95	94	84	107	58	52	96	586

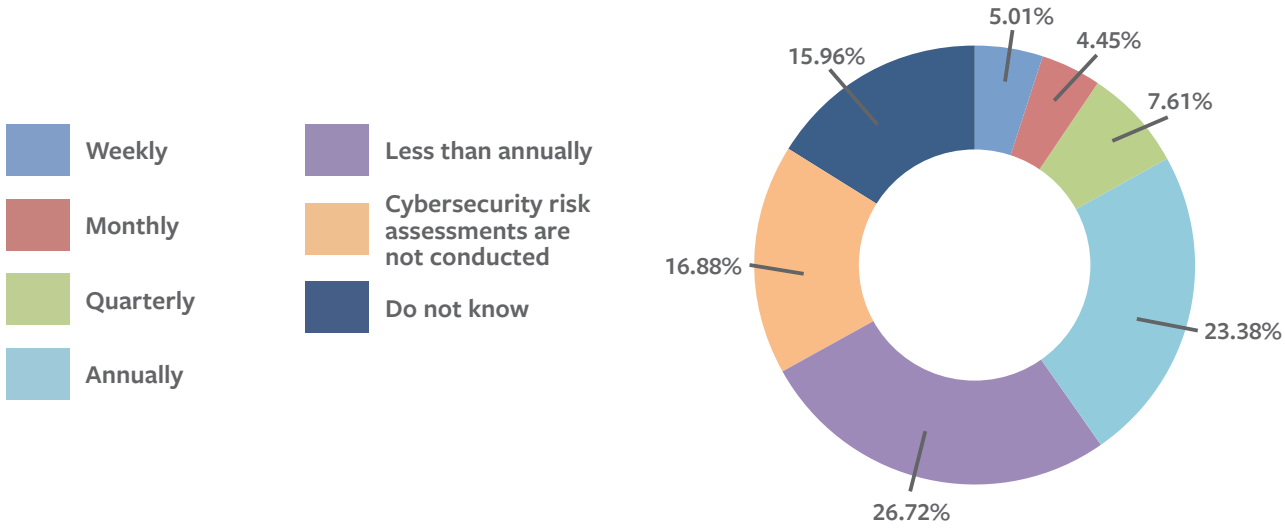
Figure 2: Water Utilities Spend Even Less on OT Cybersecurity

Percentage of 2021 Utility Budget Allocated for OT Cybersecurity	Number of Individuals Served							
	≤500	501–3,300	3,301–10,000	10,001–50,000	50,001–100,000	100,001–250,000	>250,000	Total
<1%	62	54	40	39	26	14	28	263
1%–5%	8	19	14	26	15	15	26	123
6%–10%	0	0	3	10	2	5	9	29
>10%	1	1	3	0	0	2	3	10
N/A; OT cybersecurity is managed at the municipal/county government level	5	3	3	8	3	3	0	25
Do not know	19	17	21	25	12	13	30	137
Total	95	94	84	108	58	52	96	587

Smaller budgets also translate into fewer employees focused on IT and OT security. More than 70 percent of surveyed utilities reported having less than three full-time equivalent (FTE) personnel dedicated to IT cybersecurity, and 73 percent reported having less than three FTE employees dedicated to OT security.[38] Moreover, only 30 percent of utilities reported having a chief information security officer or the equivalent.[39] Without trained personnel, it is challenging for a utility to act on information provided by the government about active threats. With a limited staff and budget, a utility's wherewithal to respond and recover from an attack is likewise hampered.

Small budgets also mean that water utilities conduct risk assessments infrequently, rarely test their cybersecurity incident response plans, and provide limited cybersecurity training to staff. Only 17 percent of respondents reported that their organization conducts cyber risk assessments more than once per year (see Figure 3).[40] Only 25 percent reported participating in cybersecurity-related tabletop exercises, mock drills, technology failure exercises, or emergency management exercises.[41]

Figure 3: Frequency of Cybersecurity Risk Assessments



This is a problem from a statutory perspective. The America's Water Infrastructure Act (AWIA) of 2018 requires community water systems serving more than 3,300 people to periodically conduct and update risk and resilience assessments (RRAs) and emergency response plans (ERPs). The RRAs must include an evaluation of "the risk to the system from malevolent acts and natural hazards," as well as an evaluation of "the resilience of … the electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system." Utilities are then required to update or develop an ERP that includes "strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system."[42] These RRAs and ERPs are effective only if the utilities have informed cybersecurity personnel who can conduct the review and take actions to mitigate the risks.

38. Ibid., page 8.
39. Ibid., page 16.
40. Ibid., page 9.
41. Ibid., page 20.
42. America's Water Infrastructure Act of 2018, Pub. L. 115-270, 132 Stat. 3765, codified as amended at 33 U.S.C. §2201. (https://www.congress.gov/115/bills/s3021/BILLS-115s3021enr.pdf)

AWIA does not require the use of a specific process to conduct the RRA or ERP, but Congress did authorize the EPA to "recognize technical standards that are developed or adopted by third party organizations or voluntary consensus standards to carry out the objectives or activities required … as a means of satisfying the requirements."[43] However, the EPA does not provide water utilities with "designated standards, methods or tools" to conduct the RRAs or to prepare ERPs and has not recognized third-party or consensus standards or guidance consistent with AWIA's intent.[44] This leads to a lack of clarity for the utilities that do conduct RRAs and create ERPs. The American Water Works Association (AWWA) has developed guidance based on the National Institute of Standards and Technology's (NIST's) Cybersecurity Risk Framework, but only 50 percent of utilities reported using that guidance.[45] Taken together, this means that many water utilities may not be aware of their cybersecurity shortfalls, and their ERPs may not mitigate their cyber risks. Remarkably, AWIA does not require that the RRAs or ERPs be submitted to the EPA for review.

Meanwhile, a majority of water utilities have not identified all of their networked IT and OT assets. As the joint WaterISAC-WSCC report notes, "An organization cannot protect what it cannot see."[46] While many large utilities reported having identified all their networked assets, that percentage drops precipitously as the size of the utility decreases.[47] Compounding this shortcoming, the EPA's guidance does not establish a baseline for normal network activity. If a company does not know what normal looks like, it will not be able to identify abnormal activity linked to a cyber breach.[48]

Despite its failures, the sector recognizes that it needs to better protect America's water infrastructure from cybersecurity threats. Survey respondents confirmed needing technical assistance and assessments, federal grants and loans, and funding to hire cybersecurity personnel, conduct training and education, and access more cybersecurity threat information.

Bureaucratic Malaise

The water sector's needs from the government mirror the responsibilities Congress assigned to the EPA and other federal agencies in the National Defense Authorization Act for Fiscal Year 2021.[49] In line with recommendations from the Cyberspace Solarium Commission (CSC), that law expanded the responsibilities of what were previously known as Sector Specific Agencies (SSAs), dubbing them sector risk management agencies (SRMAs). As a result, the EPA is now responsible for:

43. Ibid.
44. U.S. Environmental Protection Agency, "Third-Party Standards: America's Water Infrastructure Act: Risk Assessments and Emergency Response Plans," accessed November 9, 2021. (https://www.epa.gov/waterresilience/awia-section-2013)
45. Author interviews with WaterISAC and WSCC regarding survey results, July 2021.
46. "Water and Wastewater Systems Cybersecurity 2021 State of the Sector," *Water Sector Coordinating Council*, June 2021, page 13. (https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf).
47. Ibid.
48. Georgianna Shea, "Comparison of Cybersecurity Guidance for Critical Infrastructure Sectors," *Foundation for Defense of Democracies*, July 22, 2021. (https://www.fdd.org/analysis/2021/07/22/comparison-of-cybersecurity-guidance-for-critical-infrastructure-sectors)
49. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388. (https://www.congress.gov/bill/116th-congress/house-bill/6395)

- establishing programs to help the water sector identify, understand, and mitigate threats, vulnerabilities, and risks;
- recommending security measures to mitigate the consequences of destruction, compromise, and disruption of water systems;
- identifying, assessing, and prioritizing physical and cyber risks to the water sector;
- serving as the "day-to-day Federal interface" with industry;
- facilitating the exchange of information and intelligence between the water sector and the federal government to ensure both are aware of threats and vulnerabilities;
- supporting incident management and restoration efforts following a cyber breach;
- working with the water sector on emergency preparedness and response plans for natural and man-made disasters (including terrorism and cyberattacks); and
- coordinating with other federal agencies as well as state and local entities.

The Government Accountability Office (GAO) assessed the EPA's performance as an SSA multiple times over the past decade and identified a number of shortcomings. In a June 2021 letter to the EPA administrator, for example, the GAO reported that three years after it gave the EPA a series of recommendations to strengthen water infrastructure cybersecurity, the EPA still had not developed a method to evaluate the sector's adoption of cybersecurity best practices.[50] The CSC likewise noted in its March 2020 report that the EPA failed to "conduct … risk management assignments effectively."[51] Unless the EPA better prioritizes and resources this task, that gap will likely grow as the agency assumes new responsibilities as an SRMA.

Over the past 20 years, the EPA has not been organized or resourced to identify, develop, and support the necessary cybersecurity practices, resources, and tools that the water sector needs to succeed. The agency provides awareness and training briefs to only a small portion of the sector each year. This shortcoming is not, however, for lack of authority to do more. The EPA's cybersecurity mandate traces back to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which made the EPA administrator responsible for ensuring that the information and cybersecurity systems for drinking water and wastewater treatment facilities cannot be disrupted by terrorists or other groups.[52] The following year, the administration of President George W. Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which identified the water sector (and others) as critical infrastructure and tasked the EPA with supporting the water sector as its SSA.[53] In support of all SSAs, the Department of Homeland Security issued a "National Infrastructure Protection Plan" in 2006, designed to set the standard for each of the seven SSAs designated in HSPD-7.[54] When President Barack Obama issued Presidential Policy Directive 21 in 2013, designating 16 critical

50. Gene Dodaro, U.S. Government Accountability Office, "Priority Open Recommendations: Environmental Protection Agency," *Letter to Environmental Protection Agency Administrator Michael S. Regan*, June 29, 2021, page 14. (https://www.gao.gov/assets/gao-21-557pr.pdf)
51. U.S. Cyberspace Solarium Commission, *Final Report*, March 2020, page 62. (https://www.fdd.org/analysis/2020/03/11/cyberspace-solarium-commission-report)
52. Public Health Security and Bioterrorism Preparedness and Response Act of 2002, §1435 (a)(5), Pub. L. 107-188, 116 Stat. 594, codified as amended at 42 U.S.C. §201. (https://www.congress.gov/107/plaws/publ188/PLAW-107publ188.pdf)
53. U.S. Cybersecurity and Infrastructure Security Agency, Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003. (https://www.cisa.gov/homeland-security-presidential-directive-7). HSPD-7 originated the SSA designation.
54. U.S. Department of Homeland Security, "National Infrastructure Protection Plan," January 2006. (https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf)

infrastructure sectors, the EPA retained its role in leading the protection of drinking water and wastewater critical infrastructure as the SSA for the water sector.[55]

The EPA's Office of Water leads the agency's water sector cybersecurity efforts and performs the functions of the SSA (and now SRMA) for the water and wastewater systems sector. Two other EPA offices assist in this effort: the Office of Homeland Security, which works with the intelligence community to facilitate information sharing, threat awareness, and intelligence to alert water organizations of potential or actual cyberattacks against water infrastructure; and the Office of Research and Development, which seeks to improve water utilities' ability to prepare for and respond to all hazardous incidents that threaten public health.

The Office of Water includes a cybersecurity element staffed by a handful of employees.[56] The office is vastly under-resourced for the tasks expected of an SRMA for a sector with nearly 70,000 utilities serving a total of 360 million customers. In its fiscal year 2021 budget summary, the EPA noted plans to conduct cybersecurity trainings for 200 water and wastewater utilities out of those 70,000.[57] The EPA's fiscal year 2022 budget request calls for "exercises and technical support to about 1,500 water utilities, state officials, and federal emergency responders" to address both natural and man-made disasters. The Office of Water's total budget request for fiscal year 2022 is only $15.3 million, which is intended to cover not only the office's Cybersecurity mission but also its Natural Disaster and General Preparedness mission and its Water Security Initiative — an effort to identify and respond to water contamination threats in high-risk cities.[58] The equivalent office in the Department of Energy — the Office of Cybersecurity, Energy Security and Emergency Response — is led by a Senate-confirmed assistant secretary of energy and has requested a $201 million budget for fiscal year 2022.[59]

The EPA's lack of focus on cybersecurity starts at the top, as it has during both Democratic and Republican administrations. The current administrator, Michael Regan, did not raise the issue of cybersecurity at his nomination hearing on February 3, 2021, days before the Oldsmar hack, and no senator asked about it.[60] At a post-Oldsmar budget hearing before the Senate Committee on Environment and Public Works, Regan used the word "cyber" only twice in two hours.[61] He used it only once the following day during the House Energy and Commerce

55. The White House, Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

56. Three programs (Natural Disasters and Defense Preparedness, Water Security Initiative, and Cybersecurity) shared a budget of $10.3 million last year. U.S. Environmental Protection Agency, "United States Environmental Protection Agency Fiscal Year 2022 Justification of Appropriation Estimates for the Committee on Appropriations, Tab 03: Science and Technology," May 2021. (https://www.epa.gov/system/files/documents/2021-07/fy22-cj-03-science-technology.pdf)

57. U.S. Environmental Protection Agency, "FY 2021 EPA Budget in Brief," February 2020. (https://www.epa.gov/sites/default/files/2020-02/documents/fy-2021-epa-bib.pdf)

58. U.S. Environmental Protection Agency, "United States Environmental Protection Agency Fiscal Year 2022 Justification of Appropriation Estimates for the Committee on Appropriations," May 2021, page 42. (https://www.epa.gov/sites/default/files/2021-05/documents/fy-2022-congressional-justification-all-tabs.pdf)

59. U.S. Department of Energy, "Department of Energy FY 2022 Congressional Budget Request," June 2021. (https://www.energy.gov/sites/default/files/2021-06/doe-fy2022-budget-in-brief-v4.pdf)

60. U.S. Senate Committee on Environment and Public Works, "Hearing on the Nomination of Michael Regan to be Administrator of the Environmental Protection Agency," February 3, 2021. (https://www.epw.senate.gov/public/index.cfm/hearings?ID=D825A7BE-3D52-4651-9664-A373EB3699A5)

61. U.S. Senate Committee on Environment and Public Works, "Hearing on the Fiscal Year 2022 Proposed Budget for the U.S. Environmental Protection Agency," April 28, 2021. (https://www.epw.senate.gov/public/index.cfm/2021/4/hearing-on-the-fiscal-year-2022-proposed-budget-for-the-u-s-environmental-protection-agency)

Committee's three-hour budget hearing.[62] Regan was not present at the White House Cybersecurity summit on August 25, even though there was a panel on critical infrastructure cybersecurity in the energy, financial, and water sectors, with water utilities participating.[63]

Absent a well-funded and mission-focused EPA, the WaterISAC and water sector associations have worked to fill the void. The WSCC Cyber Security Working Group, supported by the AWWA, produced a "Roadmap to Secure Control Systems in the Water Sector," released in March 2008[64] and updated in 2013 and 2017.[65] The roadmap aimed to develop and implement security programs and support the conduct of risk management by utilities. These industry groups also provide web-based and online training efforts, offer a comprehensive library of technical documents, and suggest best practices for water and wastewater utilities. While the work of these industry groups is valuable, it does not absolve the EPA of its role in managing cybersecurity risk for the water sector.

Recommendations

Government and industry must work together to improve the water sector's cybersecurity. This will require enhanced public-private collaboration, expanded assistance from the federal government, and increased federal oversight of the sector. Congressional oversight can help create accountability and ensure that the EPA provides meaningful support to the water sector.

Given the size and diversity of the sector, government and industry will need to tailor their implementation of the following recommendations to the varying size, complexity, and maturity of the individual utilities affected.

Recommendations for Government

1. Resource and Empower the EPA to Succeed as an SRMA

While some SRMA responsibilities can be shared or coordinated with other federal agencies, such as CISA, the EPA retains most SRMA responsibilities. For the EPA to better fulfill these responsibilities, Congress needs to increase appropriations for the Office of Water. The EPA's fiscal year 2022 budget request includes a $4 million increase for disaster management and cybersecurity programs within its Office of Homeland Security.[66] This increase is a start but is insufficient. The Office of Water needs a substantial increase in order to meet its most basic SRMA requirements.

62. U.S. House Committee on Energy and Commerce, "Hearing on 'The Fiscal Year 2022 EPA Budget,'" April 29, 2021. (https://energycommerce.house.gov/committee-activity/hearings/hearing-on-the-fiscal-year-2022-epa-budget)
63. The White House, "Background Press Call by Senior Administration Officials on the President's Upcoming Cybersecurity Meeting," August 24, 2021. (https://www.whitehouse.gov/briefing-room/press-briefings/2021/08/25/background-press-call-by-senior-administration-officials-on-the-presidents-upcoming-cybersecurity-meeting)
64. "Roadmap to Secure Control Systems in the Water Sector," *Water Sector Coordinating Council Cyber Security Working Group*, March 2008. (https://apps.dtic.mil/sti/pdfs/ADA529983.pdf)
65. "Roadmap to a Secure and Resilient Water and Wastewater Sector," *Water and Wastewater Sector Strategic Roadmap Work Group*, May 2017. (https://www.waterisac.org/sites/default/files/public/2017_CIPAC_Water_Sector_Roadmap_FINAL_051217.pdf)
66. U.S. Environmental Protection Agency, "Fiscal Year 2022: Justification of Appropriation Estimates for the Committee on Appropriations," May 2021, page 47. (https://www.epa.gov/sites/default/files/2021-05/documents/fy-2022-congressional-justification-all-tabs.pdf)

The treatment of DOE's Office of Cybersecurity, Energy Security and Emergency Response provides a template. In addition to the department's $201 million annual budget, the Infrastructure Investment and Jobs Act of 2021 provides DOE with additional cybersecurity funding, including $50 million for modeling and assessing energy infrastructure risk and $250 million to develop advanced cybersecurity applications and technologies for the energy sector.[67] While the EPA is not currently resourced to execute or manage such programs, these are programs the agency should eventually be able to replicate.

In determining appropriate EPA funding, Congress should ensure that the agency is resourced to:

- develop active public-private collaboration with the WaterISAC and the various water associations to produce and deliver improved cybersecurity awareness training, vulnerability assessment tools, and low-cost cybersecurity solutions;
- administer a significant number of grants and low-interest loans focused on cybersecurity;
- work with the water sector to develop improved cybersecurity guidelines; and
- coordinate with other federal agencies that also support water utilities, including CISA, DOE, and the Department of Agriculture.

Based on the funding enjoyed by similar agencies that serve as SRMAs, and to fund an expansion of the EPA's staff by up to 50 personnel, the agency's cybersecurity and disaster management budget should be significantly increased to as much as $45 million a year.[68]

2. Direct Some of the EPA's Water Sector Grant Programs Exclusively Toward Cybersecurity

Today, the EPA provides grants and low-interest loans to state, local, tribal, and territorial (SLTT) governments for water and wastewater infrastructure through the Clean Water State Revolving Fund (SRF) program and Drinking Water SRF program. Through a partnership between the EPA and SLTT governments, these two programs fund a wide array of water infrastructure projects.[69] The Clean Water SRF program currently funds 11 types of infrastructure projects, including technical assistance program loans for small- and medium-sized utilities.[70] The principal goals are to facilitate compliance with national drinking water regulations and to advance the public health protection objectives of the Safe Drinking Water Act.[71] The Infrastructure Investment and Jobs Act of 2021 increased funding for these two SRFs to $14.65 billion each over the next five years.[72]

67. Infrastructure Investment and Jobs Act, §40125, H.R. 3684, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/3684/text)
68. Author interviews with industry experts, April–August 2021.
69. U.S. Environmental Protection Agency, "Water Utility Resources for the COVID-19 Pandemic," March 30, 2021. (https://www.epa.gov/coronavirus/water-utility-resources-covid-19-pandemic)
70. U.S. Environmental Protection Agency, "Learn about the Clean water State Revolving Fund (CWSRF)," July 3, 2021. (https://www.epa.gov/cwsrf/learn-about-clean-water-state-revolving-fund-cwsrf#eligibilities)
71. U.S. Environmental Protection Agency, "2017 Drinking Water State Revolving Fund Handbook," June 2017. (https://www.epa.gov/dwsrf/dwsrf-eligibilities)
72. Infrastructure Investment and Jobs Act, §50210 and §50102, H.R. 3684, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/3684/text)

Historically, the EPA has provided SRF awards for projects to improve drinking water treatment, repair and replace aging systems, and remove lead service lines.[73] Cybersecurity investments, however, represent less than 1 percent of these grants, although the EPA does not provide official statistics on this.[74] The EPA and SLTT governments should be encouraged and, if needed, mandated to prioritize cybersecurity projects in future SRF awards.

Congress should also establish a cybersecurity-specific EPA grant and low-interest loan program for water utilities. For comparison, DOE already funds numerous cybersecurity-specific grant programs, and a provision in the Infrastructure Investment and Jobs Act of 2021 provides $250 million in funding for a new DOE program, the "Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program," to help utilities protect against, detect, respond to, and recover from cybersecurity threats.[75]

The Drinking Water and Wastewater Infrastructure Act of 2021, which Congress incorporated into the Infrastructure Investment and Jobs Act of 2021, is one potential way to direct EPA grant and loan programs explicitly toward cybersecurity initiatives.[76] Specifically, the act creates $3.26 billion in new appropriations for 21 water sector grant programs and authorizes and appropriates $29.3 billion in Drinking Water and Clean Water SRF grants and loans (as noted above). The act includes a $250 million (over five years) Drinking Water program to increase resilience to natural disasters, extreme weather events, and cybersecurity vulnerabilities, as well as a $125 million (over five years) Clean Water program to increase resilience to natural disasters, extreme weather, drought, sea level rise, and cybersecurity vulnerabilities. While the act has the potential to fund cybersecurity issues, it places cybersecurity in direct competition with other, higher-priority challenges. Despite clear indications that lumping cybersecurity in with other issues has not worked in the past, the act creates no funding opportunities exclusively dedicated to addressing cyber vulnerabilities in the water sector (as it does for the energy sector).

3. Increase Funding for Rural Water Cybersecurity Programs

In 1980, the U.S. Department of Agriculture (USDA), together with the National Rural Water Association (NRWA), established the Rural Water Circuit Rider program to provide training and technical expertise to water stakeholders in rural communities. Currently, 147 circuit riders service 49 state rural water associations and Puerto Rico.[77] While the program provides vital assistance to small water organizations, the circuit riders are not equipped to provide cybersecurity-specific support to help small water and wastewater organizations bolster their defenses.

The USDA should expand the Circuit Rider Program to provide technical cybersecurity assistance. Congress should increase funding to provide for 50 cybersecurity circuit riders, whose efforts should include rapidly assessing the cybersecurity of all small water utilities, developing protocols to enhance cyber defenses, providing assistance to supplement inadequate cyber protection plans, and documenting and reporting the state of cyber protection for

73. U.S. Environmental Protection Agency, Clean Water State Revolving Fund, "2019 Annual Report: Building the Project Pipeline," September 2020. (https://www.epa.gov/sites/default/files/2020-10/documents/2019_cwsrf_annual_report_9-10.pdf)
74. Author interviews with executives representing the water and wastewater industry, May–October 2021.
75 Infrastructure Investment and Jobs Act, §40124, H.R. 3684, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/3684/text)
76. Drinking Water and Wastewater Infrastructure Act of 2021, S. 914, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/senate-bill/914/text)
77. "Circuit Rider Program," *National Rural Water Association*, accessed August 26, 2021. (https://nrwa.org/circuit-rider-program)

all small water supplies.[78] The NRWA estimates that this will require additional appropriations of about $5 million per year, and that because this is a roving program, Congress can expect a high return on investment.[79]

Similarly, the USDA and EPA have funded the Rural Community Assistance Program (RCAP), a network of non-profit organizations providing technical assistance, training, resources, and support to rural communities across the United States. RCAP provides technical assistance and training — including system assessments, personnel training, long-range planning, and grant opportunity identification — to well operators, drinking water utilities, and wastewater utilities in numerous areas. Congress should expand USDA and EPA funding for RCAP to encompass more explicit investment in cybersecurity training and technical assistance programs.

4. Direct CISA to Increase Its Support for the Water Sector

CISA is the federal government's national risk manager, providing support to all SRMAs and working to coordinate across all sectors. As part of this role, CISA leads cyber incident response, providing technical assistance to affected entities. CISA also provides steady state support to federal agencies, municipalities, and the private sector through its cybersecurity division, infrastructure security division, national risk management center, and integrated operations division. This support includes providing threat information, cybersecurity warnings, assessment tools, and other risk reduction products. While few of these products are tailored to the water sector, CISA is the primary source of federal cyber-threat information for all critical infrastructure as well as the private sector.

Congress and the administration should direct CISA to increase support for the EPA and the water sector. The Infrastructure Investment and Jobs Act of 2021 directs CISA and the EPA to identify which public water systems are a "priority" for national security and public health safety. The law further tasks CISA and the EPA to jointly develop technical support plans for these priority water systems, to include vulnerability and risk assessments and penetration testing. The act provides no funding for this CISA-EPA effort, however. CISA can also help the EPA and the water associations support water utilities through vulnerability assessments and remediation, to include a water utility risk assessment guide that is scalable across a range of utility sizes.[80] Finally, CISA can also work closely with the EPA to tailor cyber alerts and threat warnings to the IT and OT systems most widely used in the water sector. Based on the cost of similar SRMA support efforts, CISA should be provided with as much as $10 million annually to support increased water-specific cybersecurity and risk assessment efforts.[81]

5. Increase Federal Government Support for Water Sector Associations

The WaterISAC works with water associations to provide situational awareness tools, assessment tools, and training products for the sector. Many of the other ISACs for critical infrastructure sectors have established supporting relationships with their SRMAs. For example, the Electricity ISAC works closely with DOE and

78. The NRWA estimates that an additional 50 circuit riders are necessary to provide the cybersecurity technical assistance necessary. Author interviews with NRWA representatives, April–August 2021.
79. Author interviews with NRWA representatives, April–August 2021.
80 Infrastructure Investment and Jobs Act, §50113, H.R. 3684, 117th Congress (2021). (https://www.congress.gov/bill/117th-congress/house-bill/3684/text)
81. Author interviews with industry experts, April–August 2021.

manages DOE-developed programs.[82] The Multi-State ISAC, which helps improve the overall cybersecurity posture of SLTT governments, is funded by CISA ($27 million requested for fiscal year 2022) to serve as a no-cost resource for situational awareness, best practices, information sharing, and operational response for SLTT and election stakeholders.[83]

The water sector needs similar support. The EPA should fund the WaterISAC (and its water association partners) to maintain and expand programs and provide tools to enhance the cybersecurity preparedness of water utilities. This program should include efforts to:

- provide advisory support regarding the development and implementation of policies, plans, and procedures for cybersecurity readiness and resilience;
- issue advisories pertaining to cybersecurity threats to the water sector;
- provide training and conduct exercises to improve cybersecurity readiness and resilience; and
- help the EPA document the overall state of the water sector's cybersecurity readiness.

In the past, AWWA has provided cybersecurity training to hundreds of small water and wastewater systems across the country through initiatives funded by the USDA and EPA (through a Training and Technical Assistance for Small Systems grant), often in collaboration with RCAP. AWWA offered the cybersecurity training content developed under these grants in a variety of formats, including in-person and virtual workshops, eLearning courses, and as part of a risk and resilience certification program for small systems. Support for sector engagement processes such as this should be continued and expanded.

Based on similar sector engagement processes, investments in water cybersecurity outreach will require as much as $10 million per year in appropriations, with grants split between the WaterISAC and water associations.[84]

Recommendations for Industry

Water utilities need to invest more in their own cybersecurity. While the federal government should help, industry associations can ensure members fully utilize existing (and oftentimes free) resources.

1. Increase Utilities' Investment in Cybersecurity Technology and Personnel

While the federal government should help address cybersecurity vulnerabilities, water utilities must fund baseline cybersecurity costs. The aforementioned water sector survey highlighted several shortfalls, including an inadequate understanding of IT and OT networks, insufficient cybersecurity personnel, deficient cybersecurity assessments, and poor participation in cyber exercises. Experts estimate that in data-driven industries (such as

82. "E-ISAC Long-Term Strategic Plan Update," *Electricity Information Sharing and Analysis Center*, October 2020. (https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC%20Long-Term%20Strategic%20Plan.pdf)

83. U.S. Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency Budget Overview: Fiscal Year 2022 Congressional Justification," March 2021. (https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2021/jun/cs2021_0105a.pdf)

84. Estimate arrived at through author discussions with WaterISAC and experts from water associations on how much support they need to provide the programs described, April–August 2021.

financial services), cybersecurity should account for 8 to 12 percent of the overall IT budget.[85] Technology research and consulting company Gartner reports that utilities spend an average of about 6 percent.[86]

Many of the most important cybersecurity investments can be cost-effective. The EPA and the water associations could assist utilities by reviewing NIST's risk framework and tailoring recommendations to water utilities, including information security measures and controls, to help owners and operators of critical infrastructure identify and manage cyber risk. Low-cost technology solutions such as password management programs and mandatory multi-factor authentication programs would achieve inexpensive but meaningful improvements in cybersecurity. Hiring dedicated personnel and improving or upgrading IT and OT hardware can be more expensive. This is where EPA-managed grants or low-interest loans dedicated to cybersecurity are crucial.

2. Increase Water Utilities' Access to Cybersecurity Training and Assessment Resources

Training and educational resources were the need most cited by respondents to the WSCC sector survey.[87] Private companies,[88] the federal government (including but not limited to the EPA),[89] the WaterISAC,[90] and AWWA provide industry with a wide range of cybersecurity training and assessment tools[91] as well as advisories and alerts.[92]

A few tools warrant mention. In addition to software that helps utilities operate efficiently,[93] AWWA provides a sector-specific Cybersecurity Tool to help water utilities adhere to the NIST Cybersecurity Framework recommended by the WSCC.[94] The tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The EPA, meanwhile, offers the Vulnerability Self-Assessment Tool Web 3.0, a web-

85. Julie Bernard and Mark Nicholson, "Reshaping the cybersecurity landscape," *Deloitte*, July 24, 2020. (https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html); Kim Crawley, "Cybersecurity budgets explained: how much do companies spend on cybersecurity?" *AT&T Cybersecurity*, May 5, 2020. (https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget)

86. Samantha Schwartz, "Security accounts for just 5.7% of IT spend: Gartner," *Cybersecurity Drive*, October 28, 2020. (https://www.cybersecuritydive.com/news/security-budget-gartner/587911)

87. "Water and Wastewater Systems Cybersecurity 2021 State of the Sector," *Water Sector Coordinating Council*, June 2021, page 5. (https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_of_the_Industry-17-JUN-2021.pdf)

88. See, for example: "Industrial Control Systems Certifications," *Global Information Assurance Certification*, accessed August 26, 2021. (https://www.giac.org/certifications/industrial-control-systems); Robert M. Lee, "ICS515: ICS Active Defense and Incident Response," *SANS Institute*, accessed August 26, 2021. (https://www.sans.org/cyber-security-courses/industrial-control-system-active-defense-and-incident-response); Justin Searle,"ICS410: ICS/SCADA Security Essentials," *SANS Institute*, accessed August 26, 2021. (https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials)

89. See, for example: CISA's Cybersecurity Evaluation Tool and NIST's Special Publication 800-82: U.S. Cybersecurity and Infrastructure Security Agency, "Cyber Security Evaluation Tool (CSET)," accessed November 15, 2021. (https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr); U.S. Department of Commerce, National Institute of Standards, Special Publication 800-82 Rev. 2, "Guide to Industrial Control Systems (ICS) Security," May 2015. (https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final)

90. "WaterISAC Resource Center," *WaterISAC*, accessed August 26, 2021. (https://www.waterisac.org/resources)

91. For example, Jeff Szabo and John Hall, U.S. Environmental Protection Agency, "Water Security Test Bed Experiments at the Idaho National Laboratory," April 2016. (https://cfpub.epa.gov/si/si_public_record_report.cfm?Lab=NHSRC&dirEntryId=322581)

92. U.S. Cybersecurity and Infrastructure Security Agency, "ICS-CERT Alerts," accessed August 26, 2021. (https://us-cert.cisa.gov/ics/alerts)

93. "AWWA Free Water Audit Software Version 6 – Evolutions," *American Water Works Association*, December 4, 2020. (https://www.awwa.org/Portals/0/AWWA/Nosearch/Release_Memo_v6.0.pdf?ver=2020-12-02-161533-623)

94. "AWWA Resources on Cybersecurity: Cybersecurity Guidance & Tool," *American Water Works Association*, accessed September 27, 2021. (https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance)

enabled tool to help drinking water and wastewater utilities of all sizes conduct risk and resilience assessments. This tool was the product of public-private collaboration based on the "American National Standards Institute/ AWWA J100 Standards for Risk and Resilience Management."[95]

The WaterISAC and water associations should continue to ensure that members are aware of and take advantage of these resources. Smaller utilities — including their non-cybersecurity personnel, who may quickly have to become cyber incident responders in the event of a breach — may not know how to access these tools and resources.

Recommendations for Government and Industry Together

1. Establish a Joint Industry-Government Cybersecurity Oversight Program

The most dramatic way to improve the cybersecurity readiness of water utilities would be for Congress to establish a body tasked with regulating cybersecurity in the sector, similar to the role that the Federal Electricity Regulatory Commission (FERC) plays in the electricity subsector. Congress could designate the EPA as the principal federal oversight agency, with technical support provided by CISA and DOE given their demonstrated technical expertise. In the electricity subsector, FERC is paired with the North American Electric Reliability Corporation (NERC), an industry-created non-profit body that develops cybersecurity standards and other requirements. NERC follows a "defense-in-depth" strategy that incorporates three types of standards:[96]

- performance-based standards that identify outcomes to achieve;
- risk-based standards that outline requirements to address vulnerabilities that could materially compromise a system if not properly addressed; and
- competency-based standards that define a baseline set of capabilities an organization needs to meet to demonstrate its ability to perform its reliability functions.

This dramatic move is not yet realistic for the water sector, as the EPA and industry have not developed comprehensive standards related to reliability and security, and since the water sector has no body equivalent to the NERC. Without a NERC-like body in place, it would be difficult to escalate straight to a FERC model.[97]

It would be more effective for Congress to start by creating a joint industry-government cybersecurity oversight program for the water sector. Funded through congressional appropriations, the oversight function would be led by the EPA, with technical support from CISA and DOE and with industry managing the standards development process.[98] A possible framework for this approach could include:

95. U.S. Environmental Protection Agency, "Conduct a Drinking Water or Wastewater Utility Risk Assessment: Vulnerability Self-Assessment Tool – Web Enabled (VSAT Web) 3.0," accessed September 27, 2021. (https:// https://toolkit.climate.gov/tool/vulnerability-self-assessment-tool-vsat)

96. "Results Based Standards," *North American Reliability Corporation*, accessed September 28, 2021. (https://www.nerc.com/pa/Stand/Pages/ResultsBasedStandards.aspx)

97. "Frequently Asked Questions," *North American Electric Reliability Corporation*, August 2013. (https://www.nerc.com/AboutNERC/Documents/NERC%20FAQs%20AUG13.pdf); "About NERC," *North American Electric Reliability Corporation*, accessed September 28, 2021. (https://www.nerc.com/AboutNERC/Pages/default.aspx)

98. Paul Stockton, "Strengthening the Cyber Resilience of America's Water Systems: Industry-Led Regulatory Options," *American Water Works Association*, August 27, 2021, page 2. (https://www.awwa.org/Portals/0/AWWA/Government/STRENGTHENINGTHECYBERRESILIENCEOFAMERICASWATERSYSTEMS-INDUSTRY-LEDREGULATORYOPTIONS.pdf)

- developing water sector cybersecurity standards, leveraging applicable standards from NERC-Critical Infrastructure Protection for new water sector regulations;
- holding public meetings to discuss prospective regulations, consulting relevant interagency stakeholders and the intelligence community to prioritize threats, and submitting prospective standards for public comment and refinement; and
- establishing a risk-based approach to compliance auditing and enforcement functions for noncompliance with adopted standards.

In addition, the oversight body would be responsible for supporting ongoing industry-led efforts to develop strategies to mitigate vulnerabilities in networks across the water sector. In August 2021, AWWA published a comprehensive study that examined the creation of a Water Risk & Resilience Organization (WRRO) to lead a co-regulatory approach to managing cyber risks in the water sector.[99] The study recommends that Congress authorize the EPA to:[100]

- task the WRRO with developing a minimum set of cybersecurity performance standards;
- support the WRRO in drafting standards by providing technical assistance and access to threat information and by coordinating access to the Department of Homeland Security, the U.S. intelligence community, and other federal agencies;
- improve access to cyber-threat information and analysis;
- review standards proposed by the WRRO and either approve them or require the WRRO to revise and resubmit these standards; and
- establish enforcement-related activities and penalty guidelines for noncompliance.

The AWWA study merits careful review. Dr. Samantha Ravich, who serves as a CSC commissioner and as chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, has similarly suggested that the water industry "create a non-governmental, self-regulatory organization to develop and enforce mandatory cybersecurity standards for water utilities."[101] While it may take several years of investment and collaboration to build a successful joint industry-government standards and oversight regime, this effort should begin as soon as possible. It will require some investment from the federal government to get the partnership started. An appropriation split evenly over two years would expedite operationalization of this proactive co-regulatory model for managing cyber risks in the water sector. When a study coming from industry is asking for partnership with government to help implement standards and regulations, government should take note and respond favorably.

99. Paul Stockton, "Strengthening the Cyber Resilience of America's Water Systems: Industry-Led Regulatory Options," *American Water Works Association*, August 27, 2021. (https://www.awwa.org/Portals/0/AWWA/Government/STRENGTHENINGTHECYBERRESILIENCEOFAMERICASWATERSYSTEMS-INDUSTRY-LEDREGULATORYOPTIONS.pdf)
100. Ibid., page 4.
101. Samantha Ravich, "Hackers Threaten our Water Supply," *RealClearPolicy*, June 17, 2020. (https://www.realclearpolicy.com/articles/2020/06/17/hackers_threaten_our_water_supply_496397.html)

2. Amend the American Water Infrastructure Act and Use It to Increase the Cybersecurity Effectiveness of Water and Wastewater Utility Risk Assessments

AWIA requires water utilities serving more than 3,300 customers to conduct RRAs and develop ERPs. However, AWIA misses several key opportunities. The current AWIA regime does not provide assessment formats for utilities to identify specific cybersecurity standards as benchmarks, nor does it require the RRAs and ERPs to be submitted to the EPA. Additionally, AWIA does not provide a vehicle for EPA funding to help water utilities remediate discrepancies identified in their RRAs or ERPs. Finally, AWIA does not require wastewater utilities to conduct similar RRAs or ERPs. Addressing each of these four issues via amendments to AWIA would improve cybersecurity in the water sector. Specific cybersecurity standards could come from the work of the WRRO or from an independent industry-led standards recommendation effort.

The increased appropriations recommended above could fund the development of AWIA assessment formats and cybersecurity standard-setting efforts. Additionally, the cybersecurity-specific grants previously recommended for water utilities could be prioritized to fund the risk mitigation issues identified by the water utilities in their RRAs and ERPs.

Conclusion

The cybersecurity of the water sector is a weak link in U.S. national infrastructure, imperiling health and human safety, national security, and economic stability. It is critical that the United States develop an effective public-private collaboration that ensures reliable, resilient water infrastructure. This will require action and investment both by water utilities and by the federal government.

RADM (Ret.) Mark Montgomery is senior director of the Center on Cyber and Technology Innovation (CCTI) at the Foundation for Defense of Democracies (FDD). **Trevor Logan** is a research analyst at CCTI. FDD is a Washington, DC-based, nonpartisan research institute focusing on national security and foreign policy.