LIS 6107 Final Project- Issue Analysis Paper

Name Solomon Neas

Topic: Critical Infrastructure – Waste and Wastewater Systems

Issue: Cyber intrusions targeting internet-connected control systems in U.S. water and wastewater utilities pose significant risks to public safety and national security.

Paper Title: Securing U.S. Water and Wastewater Utilities: Cyber Risks, OT Exposure, and National Security Implications

BLUF

U.S. Water and Wastewater Systems (WWS) utilities face significant cyber threats from adversaries seeking to disrupt critical operations. These actors exploit vulnerabilities in internet-connected operational technology (OT) and common security weaknesses, such as inadequate identity and access management. Successful intrusions can compromise water treatment processes, directly endangering public health and safety.

Background/Context

The U.S. WWS sector provides essential services to more than 324 million Americans and underpins national security, public health, and the economy.[1] Rising cyber intrusions threaten these operations. Financially motivated criminals, nation-state actors, and hacktivists exploit systemic weaknesses across utilities.[2] State-sponsored groups, such as China's Volt Typhoon and Iran's CyberAv3ngers, have infiltrated control networks, while Russia-linked Sandworm and allied hacktivists target U.S. utilities to disrupt or damage operations.[3]

Dependence on operational technology (OT), such as Supervisory Control and Data Acquisition (SCADA) and human-machine interface (HMI) systems, exposes critical functions like chemical dosing and pump control to cyber manipulation.[4] Many utilities connect these systems to corporate networks or the internet for remote access, erasing the traditional air gap.[5]

Common weaknesses include default passwords, shared credentials, and unrevised access for former employees.[6] Flat network architecture allows lateral movement from IT to OT with minimal resistance. Intrusions into OT can alter chemical processes, disable pumps, or lock operators out of systems, forcing manual operations and risking public safety.[7] Federal agencies now describe WWS as "target-rich, cyber-poor."[8]

Key Points/Discussion

Systematic Constraints

The U.S. WWS sector is inherently fragmented and decentralized, comprising over 50,000 community water systems.[9] Most systems serve fewer than 10,000 residents.[10] This decentralized structure creates the "target-rich, cyber-poor" environment where small utilities often lack dedicated cybersecurity personnel, budget, or technical capability to secure OT environments.[11] Despite federal mandates under the Safe Drinking Water Act (SDWA) Section 1433 requiring utilities to assess cybersecurity risks, the Environmental Protection Agency (EPA) found that over 70% of inspected systems violate basic requirements.[12] This structural deficiency leaves thousands of smaller utilities highly exposed, with minimal ability to detect, respond to, or recover from cyber intrusions.[13]

Exploitation of Common Vulnerabilities

Adversaries exploit fundamental weaknesses resulting from these systematic gaps.[14] Common vulnerabilities include flat IT/OT network architectures, internet-exposed SCADA systems, and poor identity and access management practices.[15] Many utilities still use default or shared credentials, fail to implement multi-factor authentication (MFA), and neglect routine patching of known exploited vulnerabilities (KEVs).[16] Once inside, attackers can easily pivot

from IT to OT environments due to the absence of segmentation or firewall controls.[17] These weaknesses provide low-cost, high-impact avenues for intrusion, allowing even unsophisticated actors to disrupt or manipulate treatment processes.[18]

Persistent Targeting by Malicious Actors

Adversaries intensify cyber operations against the US WWS sector to gain strategic leverage and disrupt essential services.[19] China's Volt Typhoon conducts operational preparation of the environment (OPE) by embedding persistent access within critical infrastructure networks to enable future disruption during conflict.[20] Russia's APT44 (Sandworm) executes coordinated espionage and sabotage campaigns, often amplifying its impact through affiliate pro-Russia hacktivists that target utility control systems and degrade operations.[21] Iran's CyberAv3ngers, linked to the Islamic Revolutionary Guard Corps (IRGC), attack systems using Israeli-manufactured programmable logic controllers (PLCs) as geopolitical messaging.[22] Criminal organizations and hacktivists exploit weak authentication and exposed OT assets to deploy ransomware, alter control parameters, or lock out operators.[23] Collectively, these actors exploit small and poorly defended utilities as accessible gateways, using them to project influence, test capabilities, and prepare the battlespace for broader disruption.[24]

High-Profile Incidents Underscore Sector Risk

The threat is no longer theoretical.[25] Between 2013 and 2019, the EPA documented 41 cyber incidents across U.S. water systems, compared to only three in the prior seven years.[26] In 2021, a hacker remotely accessed the Oldsmar, Florida water treatment system and attempted to increase sodium hydroxide (lye) levels to toxic concentrations.[27] In 2023, Iranian-linked CyberAv3ngers compromised Unitronics PLCs in Aliquippa, Pennsylvania, and the North Texas

Municipal Water District.[28] Russia-affiliated hacktivists accessed a SCADA system in Muleshoe, Texas, causing a water tank overflow.[29] These events highlight that small-scale attacks can have immediate public safety implications.

Cascading Impacts Amplify Threat to National Security

Cyberattacks targeting U.S. WWS produce severe cascading failures that directly threaten national security.[30] Adversaries can engineer a public health crisis by manipulating treatment processes to poison the water supply with dangerous chemical levels.[31] A loss of water pressure would immediately cripple essential services, halting critical firefighting operations and degrading the operational readiness of military bases.[32] The disruption would also cause widespread economic paralysis, halting commerce and manufacturing with an estimated daily cost of $43.5 billion.[33] Ultimately, this exploitation transforms civilian utilities into powerful vectors for strategic coercion, capable of undermining societal stability and public trust.[34]

Evolving Federal Regulatory Framework and Imperative for Resilience

Recent federal efforts are closing the resilience gap by translating national security policy into local operational capacity.[35] Mandates under the SDWA and the National Security Memorandum 22 now empower the EPA to establish and enforce minimum cybersecurity requirements for the sector.[36] To help utilities meet these new standards, CISA and the EPA are promoting critical mitigation strategies such as removing OT from the public internet, enforcing strong authentication, and implementing robust network segmentation.[37] Federal partners directly support these improvements by offering scalable, no-cost pathways, including CISA's vulnerability scanning service and the EPA's technical assistance programs, which enable water systems to build resilience and sustain operational continuity.[38]

Analysis/Perspective on the Issue and Connection to U.S. National Security

Cyber intrusions into WWS constitute a strategic threat vector capable of inflicting mass disruption without kinetic force.[39] Nation-state actors use persistent access for OPE, positioning to degrade water infrastructure during future conflict.[40] Infiltrated SCADA and HMI systems provide the capability to manipulate the treatment process or halt water flow, transforming civilian infrastructure into potential attack tools. Compromise of WWS can trigger cascading failures across healthcare, defense, energy, and food sectors. Chemical manipulation or loss of water service would generate an immediate health crisis, disable firefighting and hospital functions, and halt industrial output.[41] Economic paralysis and public panic would follow, achieving the adversary's objectives of societal destabilization.[42]

Federal oversight remains fragmented, leaving local utilities unprepared for sustained cyber pressure. Limited enforcement, outdated OT systems, and inconsistent risk assessments prevent uniform defense.[43] Adversaries continue exploiting this imbalance between national importance and local capability.[44] Strengthening regulatory enforcement, technical aid, and real-time intelligence sharing remains essential to closing the gap and preserving national resilience.[45]

Notes

1. Brian E. Humphreys and Elena H. Humphreys, "Cybersecurity of the Municipal Water Sector: Background and Issues for Congress," CRS Report R48556 (Congressional Research Service, June 3, 2025), "Summary," https://www.congress.gov/crs-product/R48556.

2. Shannon Kelleher, "Not a hypothetical": US water systems at risk from cyber attacks," *The New Lede* March 22, 2023, https://www.thenewlede.org/2023/03/not-a-hypothetical-us-water-systems-at-risk-from-cyber-attacks/.

3. U.S. Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, May 2024, https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

4. Anna Ribeiro, "New CISA and EPA guidelines aim to shield water and wastewater systems from cyber threats," *Industrial Cyber*, December 16, 2024, https://industrialcyber.co/utilities-energy-power-water-waste/new-cisa-and-epa-guidelines-aim-to-shield-water-and-wastewater-systems-from-cyber-threats/.

5. Pro-Tech Systems Group, "A Practical Guide to Water Treatment SCADA Security for Facilities," *Pro-Tech Systems Group*, August 18, 2025, "The Real-World Risks of Inadequate SCADA Cybersecurity," https://www.pteinc.com/guide-to-water-treatment-scada-security-in-2025/.

6. U.S. Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, May 2024, "EPA Inspections Identify Alarming Vulnerabilities," https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

7. TXOne Networks, "Cyber Threats to Water and Wastewater Sector," *TXOne Networks*, September 12, 2025, "A Paradigm Shift," https://www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.

8. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Environmental Protection Agency, *Water and Wastewater Sector Federal Roles and Resources for Cyber Incident Response* (Incident Response Guide, January 18, 2024), "Executive Summary," https://www.cisa.gov/news-events/news/cisa-fbi-and-epa-release-incident-response-guide-water-and-wastewater-systems-sector.

9. Umang Barman, "Protecting America's Water Systems: A Cybersecurity Imperative," *Balbix*, October 8, 2024, "Why Water Utilities Are Vulnerable," https://www.balbix.com/blog/protecting-americas-water-systems-a-cybersecurity-imperative/.

10. Lisa S. Benson, Nicole T. Carter, Elena H. Humphreys, Joseph V. Jaroscak, Julie M. Lawhorn, Anna E. Normand, Jonathan L. Ramseur, Charles V. Stern, and Megan Stubbs, *Federally Supported Projects and Programs for Wastewater, Drinking Water, and Water Supply Infrastructure*, Congressional Research Service Report R46471, September 10, 2025, "Technical Assistance for Small, Rural, and Tribal Drinking Water Systems," https://www.congress.gov/crs-product/R46471.

11. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Environmental Protection Agency, *Water and Wastewater Sector Federal Roles and Resources for Cyber Incident Response* (Incident Response Guide, January 18, 2024), "Executive Summary," https://www.cisa.gov/news-events/news/cisa-fbi-and-epa-release-incident-response-guide-water-and-wastewater-systems-sector.

12. U.S. Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, May 2024, "EPA Inspections Identify Alarming Vulnerabilities," https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

13. Thao Pham, "Cybersecurity for Small Water Systems: Why it Matters and How to Get Started," *Environmental Finance Center Network*, 2025, "Key Challenges for Small and Non-Urban Utilities," https://efcnetwork.org/cybersecurity-for-small-water-systems-why-it-matters-and-how-to-get-started/.

14. Pro-Tech Systems Group, "A Practical Guide to Water Treatment SCADA Security for Facilities," *Pro-Tech Systems Group*, August 18, 2025, "Unsecured Network Architecture," https://www.pteinc.com/guide-to-water-treatment-scada-security-in-2025/.

15. ZPE Systems, "America Water Cyberattack: Another Wake-Up Call for Critical Infrastructure," *ZPE Systems*, December 2024, "How the Attack Likely Happened," https://zpesystems.com/american-water-cyberattack-another-wake-up-call-for-critical-infrastructure/.

16. U.S. Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, May 2024, "EPA inspections Identify Alarming Vulnerabilities," https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

17. Pro-Tech Systems Group, "A Practical Guide to Water Treatment SCADA Security for Facilities," *Pro-Tech Systems Group*, August 18, 2025, "The Top 5 SCADA Vulnerabilities Lurking in Water Treatment Plants," https://www.pteinc.com/guide-to-water-treatment-scada-security-in-2025/.

18. TXOne Networks, "Cyber Threats to Water and Wastewater Sector," *TXOne Networks*, September 12, 2025, "The Past of Least Resistance: How Adversaries Compromise Water Utilities," https://www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.

19. The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22, April 30, 2024), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

20. Anna Ribeiro, "ReliaQuest reports 42% rise in ransomware attacks on utilities infrastructure," *Industrial Cyber*, December 13, 2024, "ReliaQuest detailed that in early February 2024," https://industrialcyber.co/utilities-energy-power-water-waste/reliaquest-reports-42-rise-in-ransomware-attacks-on-utilities-infrastructure/.

21. Gabby Roncone, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Luke Jenkins, Dan Perez, Lexie Aytes, Alden Wahlstrom, "Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm," *Google Cloud Blog* (Mandiant), April 17, 2024, https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm.

22. U.S. Department of the Treasury, "Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure," Press Release, February 2, 2024. https://home.treasury.gov/news/press-releases/jy2072.

23. U.S. Environmental Protection Agency and Cybersecurity and Infrastructure Security Agency, *Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems* (Joint Fact Sheet, December 13, 2024), 1, https://www.epa.gov/system/files/documents/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf.

24. TXOne Networks, "Cyber Threats to Water and Wastewater Sector," *TXOne Networks*, September 12, 2025, "The Dilemma of Water Utilities," https://www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.

25. Shannon Kelleher, "Not a hypothetical": US water systems at risk from cyber attacks," *The New Lede,* March 22, 2023, https://www.thenewlede.org/2023/03/not-a-hypothetical-us-water-systems-at-risk-from-cyber-attacks/.

26. Shannon Kelleher, "Not a hypothetical": US water systems at risk from cyber attacks," *The New Lede*, March 22, 2023, "Escalating attacks," https://www.thenewlede.org/2023/03/not-a-hypothetical-us-water-systems-at-risk-from-cyber-attacks/.

27. Brian E. Humphreys and Elena H. Humphreys, *Cybersecurity of the Municipal Water Sector: Background and Issues for Congress*, Congressional Research Service Report R48556, June 3, 2025, "Introduction," https://www.congress.gov/crs-product/R48556.

28. Nossaman eAlert. "White House Officials Want State Water/Wastewater Cybersecurity Plans Soon," *Nossaman*, April 2, 2024, https://www.nossaman.com/newsroom-insights-white-house-officials-want-state-water-wastewater-cybersecurity-plans-soon.

29. Shannon Pierson, "Slashing EPA funding may have downstream cybersecurity impacts on an already vulnerable water sector," *CLTC*, May 2025, "Nation-state Actors are Targeting US Water Infrastructure," https://cltc.berkeley.edu/publication/slashing-epa-funding-may-have-downstream-cybersecurity-impacts-on-an-already-vulnerable-water-sector/.

30. Erica Lonergan and Michael Poznansky, "A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats," *War on the Rocks*, February 25, 2025, "Two Distinct Threats," https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/.

31. Pro-Tech Systems Group, "A Practical Guide to Water Treatment SCADA Security for Facilities," *Pro-Tech Systems Group*, August 18, 2025, "The Real-World Risks of Inadequate SCADA Cybersecurity," https://www.pteinc.com/guide-to-water-treatment-scada-security-in-2025/.

32. Cybersecurity and Infrastructure Security Agency, "Water and Wastewater Systems," *CISA.*gov, Accessed October 19, 2025, Overview, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector.

33. U.S. Water Alliance, *The Economic Impact of Investing in Water Infrastructure* (Report, September 2023), 10, https://uswateralliance.org/wp-content/uploads/2023/09/Economic-Impact-of-Investing-in-Water-Infrastructure_VOW_FINAL_pages_0.pdf.

34. Springbrook Software. "Cybersecurity in the Water & Wastewater Sector: Securing America's Critical Infrastructure in the Age of AI," *Springbrook Software*, July 31, n.d., https://springbrooksoftware.com/cybersecurity-in-the-water-wastewater-sector-securing-americas-critical-infrastructure-in-the-age-of-ai/.

35. Jonathon Gordon, "Critical Infrastructure Protection in Modern Society," *Industrial Cyber*, May 21, 2024, "The Role of Government and Collaborative Efforts for Critical Infrastructure Protection," https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/.

36. Alexis Ward and Michael G. Gruden, "Changes to Critical Infrastructure Requirements," *Crowell & Moring LLP*, January 28, 2025, https://www.crowell.com/en/insights/publications/changes-to-critical-infrastructure-requirements.

37. U.S. Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*, May 2024, "Actions Systems Should Take Now," https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

38. Cybersecurity and Infrastructure Security Agency, Environmental Protection Agency, and Federal Bureau of Investigation, *Top Cyber Actions for Securing Water Systems* (Fact Sheet, March 2024), 1, https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf.

39. Giacomo Biggio, "Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law," *Journal of Conflict and Security Law* 30, no. 2 (2025): 241–263, https://doi.org/10.1093/jcsl/kraf008.

40. Erica Lonergan and Michael Poznansky, "A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats," *War on the Rocks*, Commentary, February 25, 2025, "Two Distinct Threats," https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/.

41. Pro-Tech Systems Group, "A Practical Guide to Water Treatment SCADA Security for Facilities," *Pro-Tech Systems Group,* August 18, 2025, "The Real-World Risks of Inadequate SCADA Cybersecurity," https://www.pteinc.com/guide-to-water-treatment-scada-security-in-2025/.

42. Shannon Kelleher, "Not a hypothetical": US water systems at risk from cyber attacks," *The New Lede*, March 22, 2023, "Wreaking havoc,"

https://www.thenewlede.org/2023/03/not-a-hypothetical-us-water-systems-at-risk-from-cyber-attacks/.

43. Brian E. Humphreys and Elena H. Humphreys, "Cybersecurity of the Municipal Water Sector: Background and Issues for Congress," CRS Report R48556 (Congressional Research Service, June 3, 2025), Introduction, https://www.congress.gov/crs-product/R48556.

44. Brian E. Humphreys and Elena H. Humphreys, "Cybersecurity of the Municipal Water Sector: Background and Issues for Congress," CRS Report R48556 (Washington, DC: Congressional Research Service, June 3, 2025), Appendixes, https://www.congress.gov/crs-product/R48556.

45. Jonathon Gordon, "Critical Infrastructure Protection in Modern Society," Industrial Cyber, May 21, 2024, "The Role of Government and Collaborative Efforts for Critical Infrastructure Protection," https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/.

Bibliography

Barman, Umang. "Protecting America's Water Systems: A Cybersecurity Imperative," *Balbix*. October 8, 2024. https://www.balbix.com/blog/protecting-americas-water-systems-a-cybersecurity-imperative/.

Benson, Lisa S., Nicole T. Carter, Elena H. Humphreys, Joseph V. Jaroscak, Julie M. Lawhorn, Anna E. Normand, Jonathan L. Ramseur, Charles V. Stern, and Megan Stubbs. *Federally Supported Projects and Programs for Wastewater, Drinking Water, and Water Supply Infrastructure*. Congressional Research Service Report R46471. September 10, 2025. https://www.congress.gov/crs-product/R46471.

Biggio, Giacomo. "Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law." *Journal of Conflict and Security Law* 30, no. 2 (2025): 241–263. https://doi.org/10.1093/jcsl/kraf008.

Cybersecurity and Infrastructure Security Agency, Environmental Protection Agency, and Federal Bureau of Investigation. *Top Cyber Actions for Securing Water Systems*. Fact Sheet. March 2024. https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf.

Cybersecurity and Infrastructure Security Agency. "Water and Wastewater Systems." Overview. Accessed October 19, 2025. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector.

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Environmental Protection Agency. *Water and Wastewater Sector Federal Roles and Resources for Cyber Incident Response*. Incident Response Guide. January 18, 2024. https://www.cisa.gov/news-events/news/cisa-fbi-and-epa-release-incident-response-guide-water-and-wastewater-systems-sector.

Gordon, Jonathon. "Critical Infrastructure Protection in Modern Society." *Industrial Cyber*, May 21, 2024. https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society/.

Humphreys, Brian E., and Elena H. Humphreys. "Cybersecurity of the Municipal Water Sector: Background and Issues for Congress." CRS Report R48556, Congressional Research Service, June 3, 2025. https://www.congress.gov/crs-product/R48556.

Kelleher, Shannon. "Not a hypothetical: US water systems at risk from cyber attacks." *The New Lede*, March 22, 2023. https://www.thenewlede.org/2023/03/not-a-hypothetical-us-water-systems-at-risk-from-cyber-attacks/.

Lonergan, Erica, and Michael Poznansky. "A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats." *War on the Rocks*. February 25, 2025. https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/.

Nossaman eAlert. "White House Officials Want State Water/Wastewater Cybersecurity Plans Soon." *Nossaman*. April 2, 2024. https://www.nossaman.com/newsroom-insights-white-house-officials-want-state-water-wastewater-cybersecurity-plans-soon.

Pham, Thao. “Cybersecurity for Small Water Systems: Why It Matters and How to Get Started.” *Environmental Finance Center Network*. 2025. https://efcnetwork.org/cybersecurity-for-small-water-systems-why-it-matters-and-how-to-get-started/.

Pierson, Shannon. “Slashing EPA funding may have downstream cybersecurity impacts on an already vulnerable water sector.” *CLTC*, May 2025. https://cltc.berkeley.edu/publication/slashing-epa-funding-may-have-downstream-cybersecurity-impacts-on-an-already-vulnerable-water-sector/.

Pro-Tech Systems Group. “A Practical Guide to Water Treatment SCADA Security for Facilities.” *Pro-Tech Systems Group*. August 18, 2025. https://www.pteinc.com/guide-to-water-treatment-scada-security-in-2025/.

Springbrook Software. “Cybersecurity in the Water & Wastewater Sector: Securing America’s Critical Infrastructure in the Age of AI.” *Springbrook Software*, July 31, n.d.. https://springbrooksoftware.com/cybersecurity-in-the-water-wastewater-sector-securing-americas-critical-infrastructure-in-the-age-of-ai/.

Ribeiro, Anna. “New CISA and EPA guidelines aim to shield water and wastewater systems from cyber threats.” *Industrial Cyber*, December 16, 2024. https://industrialcyber.co/utilities-energy-power-water-waste/new-cisa-and-epa-guidelines-aim-to-shield-water-and-wastewater-systems-from-cyber-threats/.

Ribeiro, Anna. “ReliaQuest reports 42% rise in ransomware attacks on utilities infrastructure.” *Industrial Cyber*, December 13, 2024. https://industrialcyber.co/utilities-energy-power-water-waste/reliaquest-reports-42-rise-in-ransomware-attacks-on-utilities-infrastructure/.

Roncone, Gabby, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Luke Jenkins, Dan Perez, Lexie Aytes, Alden Wahlstrom. “Unearthing APT44: Russia’s Notorious Cyber Sabotage Unit Sandworm.” *Google Cloud Blog* (Mandiant), April 17, 2024. https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm.

The White House. *National Security Memorandum on Critical Infrastructure Security and Resilience*. NSM-22. April 30, 2024. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

TXOne Networks. “Cyber Threats to Water and Wastewater Sector.” *TXOne Networks*. September 12, 2025. https://www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.

U.S. Department of the Treasury. “Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure.” Press Release. February 2, 2024. https://home.treasury.gov/news/press-releases/jy2072/.

U.S. Environmental Protection Agency and Cybersecurity and Infrastructure Security Agency. *Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems*. Joint Fact Sheet. December 13, 2024. https://www.epa.gov/system/files/documents/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf.

U.S. Environmental Protection Agency. *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*. May 2024. https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities.

U.S. Water Alliance. *The Economic Impact of Investing in Water Infrastructure*. September 2023. https://uswateralliance.org/wp-content/uploads/2023/09/Economic-Impact-of-Investing-in-Water-Infrastructure_VOW_FINAL_pages_0.pdf.

Ward, Alexis, and Michael G. Gruden. "Changes to Critical Infrastructure Requirements." *Crowell & Moring LLP.* January 28, 2025. https://www.crowell.com/en/insights/publications/changes-to-critical-infrastructure-requirements.

ZPE Systems. "American Water Cyberattack: Another Wake-Up Call for Critical Infrastructure." *ZPE Systems*, December 2024. https://zpesystems.com/american-water-cyberattack-another-wake-up-call-for-critical-infrastructure/.