Cybersecurity and Maryland's Community Water and Wastewater Systems: Analysis and Recommendations for the Maryland Cybersecurity Council

February 13, 2025

Abstract

This report offers findings and cybersecurity policy recommendations for water and wastewater systems (WWS) in Maryland, with an emphasis on community water systems. Examples of actions taken by other states are also included. While the recommendations in this report are tailored to the WWS sector, the recommendations may be useful to other sectors of critical infrastructure as well.

Matthew Mitroka, PhD, CISSP

Executive Summary[1]

This research report provides policy recommendations addressing cybersecurity challenges facing the Maryland Water and Wastewater Systems (WWS) sector, emphasizing Community Water Systems (CWS). It also provides recommendations for the WWS sector to improve cybersecurity through best practices and improved cyber awareness. The digital transformation of the WWS sector introduces an increased reliance on data, technology, and connectivity while reducing traditional segmentation between the Information Technology (IT) and Operational Technology (OT) ecosystems. This modernization seeks to increase efficiency but also creates potential vulnerabilities and increases the risk of cyberattacks.

This report highlights the following key issues:

- **Digital Transformation and Increased Cyber Threats**
- **Vulnerabilities of the Water System**
- **Barriers to Cybersecurity**
- **Lack of Comprehensive Federal Regulation**

With increased cyber threats facing the sector, it is important to increase awareness and encourage the adoption of cybersecurity among water facilities. The recommendations and best practices in this paper provide opportunities to increase cybersecurity for the WWS sector in Maryland and include:

- **Increased investment in cybersecurity training and awareness programs for water utility personnel and those along the management chain.**
- **Strengthening Maryland regulations and departments to increase cybersecurity within the WWS sector.**
- **Prioritization of cybersecurity risk assessments and mitigation strategies for water infrastructure.**
- **Advocacy for stronger cybersecurity policy at the federal level and support for water utilities in implementing cybersecurity best practices.**

While the U.S. Environmental Protection Agency (EPA) works to identify a federal strategy to enhance the security of the U.S. WWS sector, through proactive actions, Maryland should strengthen its water system's resiliency and reduce cyber risk.

---

[1] This research was conducted by Matthew Mitroka, Ph.D., a National Security Agency (NSA) State Fellow, who served for twelve months in the Office of the Attorney General in support of the Maryland Cybersecurity Council. The Council is a statutory body chaired by the Attorney General or his designee. This report and its recommendations were endorsed in their entirety by the Council's Subcommittee on Critical Infrastructure and by the Council itself. The author expresses his appreciation to the Ofifice of the Attorney General for its administrative support and to members of the Council and many others in the private sector, federal service, State government, and in the local water and wastewater sector for their help in understanding this sector.

Table of Contents

1. THE WATER AND WASTEWATER SYSTEMS (WWS) SECTOR AND INDUSTRIAL CYBERSECURITY

The U.S. Water and Wastewater Systems (WWS) sector is one of 16 critical infrastructure sectors vital to the United States. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) notes that a "reliable supply of clean drinking water and effective wastewater treatment is vital to modern life and the nation's economy." Early on, it is also instilled in our lives that water is essential for life and that humans cannot go without water for about three days. Further, "water, and specifically liquid water, is deemed so important to the creation and sustenance of life that few scientists entertain the possibility of life existing on worlds without it."[2]

Highlighting the importance of the WWS sector, Jennifer Kocher, vice president of communications and marketing for the National Water Companies Association, stressed in early 2024 that "water is the only utility that you ingest. So, if a bad actor gets into and wreaks havoc on a water system, the consequences could be very dire."[3] Protecting the WWS sector from cyberattacks is challenging. Michael S. Regan, the 16th Administrator of EPA, and Jake Sullivan, Assistant to the President for National Security Affairs, highlighted the risk in a letter to States from the White House in March 2024. They noted, "drinking water and wastewater systems are an attractive target for cyberattacks because they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices."[4]

Industry and the critical infrastructure sectors have been undergoing digital transformation as technology was introduced in the third industrial revolution and even more so with the fourth industrial revolution, also referred to as Industry 4.0. Data, automation, smart machines, Internet of Things (IoT), cloud computing, artificial intelligence (AI) and machine learning, and Information Technology (IT)-Operational Technology (OT) integration seek to improve efficiency and streamline operations. These also increase the risk of a cyber incident for the WWS sector as reliance on connectivity and data become key aspects of operations.

The digital transformation of the WWS sector creates a new set of technology and management challenges. In March 2024, Dragos CEO Robert M. Lee warned that digitalization brings greater homogeneity within critical infrastructure, which creates vulnerabilities as plants are no longer unique. These vulnerabilities are shared within and across sectors.[5] Additionally, some modern water systems cannot operate in a manual mode due to the reliance on technology, which increases the risk and impact that a cyber attack may have on a system. While this

---

[2] Ireland, Tom. 2021. "This is why water is essential for life on Earth... and perhaps the rest of the Universe." *BBC Science Focus*. 11 1. Accessed 11 7, 2024. https://www.sciencefocus.com/nature/does-all-life-need-water.

[3] Fox-Sowell, Sophia, "Where's the Federal Legislation for State Water Utility Cybersecurity?," *StateScoop* (blog), February 1, 2024, https://statescoop.com/state-water-utility-cybersecurity-federal-legislation/.

[4] Michael S. Reagan and Jake Sullivan, "Letter to Governors" (The White House, March 18, 2024), https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf.

[5] Christian Vasquez, "Dragos CEO: Digitization in Critical Infrastructure Will Spur Attacks," CyberScoop, March 6, 2024, https://cyberscoop.com/water-digitization-critical-infrastructure-attacks/.

transformation aims to improve efficiency and streamline operations, it also increases the potential cyber risk a system may face.

First, IT and OT systems are different in how they operate and what their requirements are. These systems are described as the business systems (IT) and the control systems (OT). Users of IT systems may be familiar with occasional glitches, such as a program freezing or a system crashing. While these instances can frustrate users, the results can have a minimal impact on the user via a forced restart, recovering a document, or perhaps just reloading a website. On the OT side, these systems are designed for consistent, reliable operation and control of the physical environment and processes. A glitch that takes down an OT device could dramatically impact the water system—perhaps a chemical is added at too high a rate, or untreated sewage is discharged. These impacts can have severe health consequences or downstream impacts on those relying on the water service. In contrast, IT system impacts may be more localized depending on the specific issue.

Several factors present within OT further challenge the WWS sector. Cisco highlights that initial design, ongoing maintenance, and the static nature and long lifecycles of OT equipment create common challenges.[6] Many OT devices were designed at a time when they were physically separated from IT systems and not connected to the outside world. Additionally, many OT devices were not built to comply with modern standards. They lack inherently strong security requirements and design features. As a result, legacy OT systems are vulnerable to cyber attacks when connected to a network.

Additionally, patching vulnerabilities in any system is important. However, patch management and application can be limited or non-existent within OT. A patch's impact must be assessed, tested, and ensured that it will not disrupt the system.[7] The commonly known Patch Tuesday within IT systems may be translated in some OT systems to "Patch Maybe?" as the barriers and impact to patching an OT system may not be one an operator wishes to risk. Some operators may install a system and leave it untouched over its lifecycle.

Illustrating the potential for a patch or update to have a widespread impact occurred on July 19, 2024. Although the update impacted IT systems, it demonstrated the severe impact that can result. Cybersecurity company CrowdStrike released an update to Windows systems that led to computer system crashes worldwide. As the Windows systems failed, services across many industries, including airlines, public transportation, healthcare, banks, and more, were disrupted. Insurers estimated the cost to U.S. Fortune 500 companies was $5.4 billion.[8] A critical failure similar to this in an OT system could cause even greater chaos. Imagine water systems failing across the globe if a patch were to have a similar effect. In the United States, the

---

[6] Hanes, David, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, and Jerome Henry. *IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things*. Cisco Press, 2017.

[7] Syed M. Belal, "The Top 7 Operational Technology Patch Management Best Practices," Blog, ISA Global Cybersecurity Alliance, n.d., https://gca.isa.org/blog/the-top-7-operational-technology-patch-management-best-practices.

[8] Nick Robins-Early, "CrowdStrike Global Outage to Cost US Fortune 500 Companies $5.4bn," *The Guardian*, July 24, 2024, sec. Technology, https://www.theguardian.com/technology/article/2024/jul/24/crowdstrike-outage-companies-cost.

Value of Water Campaign[9] estimated that in 2017, on average, a business lost $230 in sales per employee for every day of water disruption.[10] A one-day disruption across the U.S. would cost $43.5 billion in sales. As of late 2024, the financial impact of a major disruption would undoubtedly be higher than in 2017.

1.1 Cyber Threats

> *Operational Technology (OT) systems are becoming increasingly software-driven and connected. This creates new digitalization opportunities but can also increase the risk of cyber security breaches that can have severe consequences.[11]*

While the WWS sector transformation benefits operators and customers, those who seek to leverage technology for malicious reasons have also sought to take advantage of this transformation. Cyber threat actors across the spectrum have increasingly attempted to attack the WWS sector. In November 2023, an Iran-linked group known as "Cyber Av3ngers" attacked the Municipal Water Authority of Aliquippa, Pennsylvania, gaining control over a device.[12] Upon recognition of the incident, the plant was placed into manual operation. In April 2024, a cyber attack against the water system in Muleshoe, Texas, caused an overflow before the system was taken offline and placed into manual operation.[13]

Both attacks were against small municipalities with less than 10,000 residents. However, attacks are not against just one segment of the sector. In October 2024, American Water, the largest water utility in the U.S. with a subsidiary in Maryland, was the victim of an attack against their billing system. While American Water communicated that the water supply was uninterrupted, disruptions impacted the billing system and customer portal access.[14]

These attacks are only a few examples but highlight that the U.S. WWS sector is at risk and that the size of the system does not stop cyber threat actors from attempting to attack it. An EPA

---

[9] According to the US Water Alliance website, "The Value of Water Campaign is a coalition of leading organizations and individuals from across the US water sector who are working to educate and inspire Americans about how our water is essential, invaluable, and in need of investment." https://uswateralliance.org/programs/the-value-of-water-campaign/

[10] Value of Water Campaign, "The Economic Benefits of Investing in Water Infrastructure," 2017, https://uswateralliance.org/wp-content/uploads/2023/09/Economic-Impact-of-Investing-in-Water-Infrastructure_VOW_FINAL_pages_0.pdf.

[11] Geir Kjetil Hanssen et al., *A Continuous OT Cybersecurity Risk Analysis and Mitigation Process* (Research Publishing Services, 2023), https://doi.org/10.3850/978-981-18-8071-1_P413-cd.

[12] Christian Vasquez and AJ Vincens, "Pennsylvania Water Facility Hit by Iran-Linked Hackers," CyberScoop, November 29, 2023, https://cyberscoop.com/pennsylvania-water-facility-hack-iran/.

[13] Ken Miller, "Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow," The Texas Tribune, April 19, 2024, https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/.

[14] Ruben Rodriguez, "American Water Reactivating Systems After Cyber Event," AP News, October 15, 2024, https://apnews.com/press-release/ein-presswire-newsmatics/camden-d80e4d4bb41e95a0c64847593b34ac20.

spokesman highlighted in June 2024 that "all drinking water and wastewater systems are at risk—large and small, urban and rural."[15]

1.1.1 Geopolitics

> Critical infrastructure networks worldwide continue to be targeted by malicious cyber actors, including in conflict, where cyberspace is now an established domain of warfare and cyberattacks are used for strategic, political, economic and national security objectives.
> *-- Australian Signals Directorate[16]*

The WEF highlighted that geopolitical tensions pose significant risks to critical infrastructure. The WEF noted that ongoing conflicts affected regions beyond those directly involved in specific conflicts as nation-state threats "spillover into the cyber domain."[17] Therefore, the U.S. WWS sector, including the Maryland WWS sector, is at risk of a cyber-attack as geopolitical events turn attackers towards U.S. critical infrastructure. The Office of the Director of National Intelligence Annual Threat Assessment of the U.S. Intelligence Community noted:[18]

> If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.

In February 2024, CISA warned that People's Republic of China (PRC) state-sponsored cyber actors referred to as Volt Typhoon were pre-positioning themselves in the IT systems of U.S. critical infrastructure.[19] The warning noted that attackers could utilize these IT network accesses to move laterally into the OT networks to disrupt critical systems. The attackers often achieve lateral movement using compromised valid credentials and Remote Desktop Protocol (RDP), which allows remote desktop access and control.

China is not the only state threat actor targeting critical infrastructure in the U.S. In May 2024, the EPA issued an enforcement alert warning that cyberattacks against CWSs were increasing

---

[15] Trevor Laurence Jockims, "America's Drinking Water Is Facing Attack, with Links Back to China, Russia and Iran," CNBC, June 26, 2024, https://www.cnbc.com/2024/06/26/americas-drinking-water-under-attack-china-russia-and-iran.html.

[16] Australian Signals Directorate, "2023–2024 Cyber Threat trends For Critical Infrastructure," November 20, 2024, https://www.cyber.gov.au/sites/default/files/2024-11/2023-24-cyber-threat-trends-for-critical-infrastructure.pdf.

[17] World Economic Forum. "Global Cybersecurity Outlook 2025." Insight Report. Geneva, Switzerland, January 13, 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[18] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[19] US CISA, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Cybersecurity Advisory, February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

in frequency and targeting vulnerable water systems to manipulate OT.[20] The EPA warned that Iranian Government Islamic Revolutionary Guard Corps (IRGC)- affiliated cyber actors and pro-Russia hacktivists were targeting water infrastructure in addition to China. In 2025, experts warned that cyberattacks "will increasingly be tied to geopolitical conflicts, with commercial entities caught in the crossfire as both tactical and strategic targets."[21]

1.2 Introduction to the Maryland WWS Sector

The EPA defines a public water system (PWS) as a public or privately owned system that "provides water for human consumption through pipes or other constructed conveyances to at least 15 service connections or serves an average of at least 25 people for at least 60 days a year." These systems are further classified into three types by the timeframe they serve the population:[22]

- *Community Water System* **(CWS):** A public water system that supplies water to the same population year-round.

- *Non-Transient Non-Community Water System* **(NTNCWS)**: A public water system that regularly supplies water to at least 25 of the same people at least six months per year. Some examples are schools, factories, office buildings, and hospitals which have their own water systems.

- *Transient Non-Community Water System* **(TNCWS)**: A public water system that provides water in a place such as a gas station or campground where people do not remain for long periods of time.

The water systems of Maryland are a complex, distributed group. In 2023, 3019 water systems comprised community and non-community systems. Community water systems totaled 468, and the EPA classifies them based on the size of the population they serve. These categories are:

- Very Small: 500 or less
- Small: 501 - 3,300
- Medium: 3,301 - 10,000
- Large: 10,001 - 100,000
- Very Large: Greater than 100,000

---

[20] US EPA, "EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water," News Release, May 20, 2024, https://www.epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect.
[21] Rubinstein, Carrie. "Top Cyber Threats To Watch Out For In 2025." Forbes. Accessed December 30, 2024. https://www.forbes.com/sites/carrierubinstein/2024/12/30/top-cyber-threats-to-watch-out-for-in-2025/.
[22] US EPA, "Information about Public Water Systems," September 21, 2015, https://www.epa.gov/dwreginfo/information-about-public-water-systems.

The Breakdown of Community Water Systems in Maryland:

System Size	Number of Systems	Population Served	Population Percentage
Very Large	5	4,181,331	76.19%
Large	26	888,866	16.20%
Medium	40	225,748	4.11%
Small	105	141,528	2.58%
Very Small	292	50,526	0.92%
Total	468	5,487,999	

Representative Systems Within Target Categories:

System Size	Name	Population Served	Population Percentage
Very Large	WSSC Water	1,900,000	34.62%
	City of Baltimore	1,600,000	29.15%
Large	City of Hagerstown	92200	1.68%
	City of Frostburg	11000	0.20%
Medium	Town of Mount Airy	9890	0.18%
	Town of Centreville	3322	0.06%

For the recommendations made in this report, CWSs will be the system of focus. In discussions with the Maryland Department of the Environment (MDE) Water Supply Program, selecting to focus on CWSs in the Medium, Large, and Very Large categories is the best use of limited resources to improve security for the greatest percentage of Maryland residents and businesses. These 81 systems provide water to 96.50 percent of Maryland's population.

It is not that Small and Very Small systems are not important, and to those dependent on these systems, they are the most important systems. However, when considering systems in Maryland that rely on OT and are at the greatest risk regarding cybersecurity and cyber incidents, the three largest categories of systems are those most likely to have OT and connected technologies. Many of Maryland's Small and Very Small systems are of lesser complexity and run manually and "with a clipboard and paper." Cybersecurity awareness is still important for all systems, especially if they modernize their technology in the future.

Federal oversight of the water system in Maryland is the responsibility of the EPA via drinking water regulations.[23] The Safe Drinking Water Act (SDWA) and America's Water Infrastructure Act (AWIA) are the main regulations administered by the EPA. At the State level, laws adopted by the Maryland General Assembly and signed into law by the Governor are developed into regulations by the MDE. Most recently, AWIA was updated to require CWSs serving more than 3,300 people to conduct risk and resilience assessments (RRAs), including cybersecurity. Also, the Modernize Maryland Act of 2022 requires Maryland water and wastewater systems serving

---

[23] US EPA, "Drinking Water Regulations," September 21, 2015, https://www.epa.gov/dwreginfo/drinking-water-regulations.

10,000 or more users and receiving financial assistance from the state to conduct a cybersecurity vulnerability assessment and, if appropriate, develop a cybersecurity plan.[24]

1.3 Awaiting Federal Regulation

As of early 2025, the federal government has not implemented comprehensive regulations focused on cybersecurity for the WWS sector. According to Harrell and Le (2025), the fragmented approach hinders progress and forces cyber experts to navigate competing regulations.[25] In March 2023, the EPA released a memorandum titled "Addressing Public Water System Cybersecurity in Sanitary Surveys or an Alternate Process" that noted, "EPA's interpretation that states must include cybersecurity when they conduct periodic audits of water systems (called "sanitary surveys")."[26] Attorneys general in Missouri, Arkansas, and Iowa, as well as the American Water Works Association (AWWA) and National Rural Water Association (NRWA), challenged the EPA's method in lawsuits.[27] As a result, instead of mandating these cybersecurity measures, the EPA encouraged states to review PWS cybersecurity to address vulnerabilities voluntarily.[28]

Additionally, in August 2024, the U.S. Government Accountability Office (GAO) issued a report titled "Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems" (GAO-24-106744).[29] The GAO found that the EPA had not identified and prioritized the greatest risks to the water sector, and it relies on water systems to improve cybersecurity voluntarily. The GAO made the following recommendations for executive action:

- The Administrator of EPA should, as required by law, conduct a water sector risk assessment, considering physical security and cybersecurity threats, vulnerabilities, and consequences. (Recommendation 1)
- The Administrator of EPA should develop and implement a risk-informed cybersecurity strategy, in coordination with other federal and sector stakeholders, to guide its water sector cybersecurity programs. Such a strategy should include information from a risk assessment and should identify objectives, activities, and performance measures;

---

[24] Maryland General Assembly, "State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022)," May 11, 2022, https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/Hb1205/?ys=2022rs.

[25] Harrell, Brian, and Jeff Le. "Restoring U.S. Cyber Resilience: A Blueprint for the New Administration." *CyberScoop* (blog), January 17, 2025. https://cyberscoop.com/restoring-u-s-cyber-resilience-trump-administration-brian-harrell-jeff-le-op-ed/.

[26] US EPA, "EPA Takes Action to Improve Cybersecurity Resilience for Public Water Systems," News Release, March 3, 2023, https://www.epa.gov/newsreleases/epa-takes-action-improve-cybersecurity-resilience-public-water-systems.

[27] Andrew Bailey, Tim Griffin, and Brenna Byrd, Petition For Review, No. 23-1787 (United States Court of Appeals for the Eighth Circuit April 17, 2023). https://content.govdelivery.com/attachments/IACIO/2023/04/18/file_attachments/2470891/Iowa%20Petition%20for%20Review.pdf

[28] Jessica Lyons, "EPA Rescinds US Water Cybersecurity Rule after Legal Battle," The Register, October 13, 2023, https://www.theregister.com/2023/10/13/epa_rescinds_water_cybersecurity_rule/.

[29] US GAO, "Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems," August 1, 2024, https://www.gao.gov/products/gao-24-106744.

roles, responsibilities, and coordination; and needed resources and investments. (Recommendation 2)

- The Administrator of EPA should evaluate its existing legal authorities for carrying out EPA's cybersecurity responsibilities and seek any needed enhancements to such authorities from the administration and Congress. (Recommendation 3)
- The Administrator of EPA should submit the Vulnerability Self-Assessment Tool (VSAT) for independent peer review and revise the tool as appropriate. (Recommendation 4)

In response, the EPA planned to release the water sector risk assessment and risk management plan in January 2025. The EPA also formed The Water Sector Cybersecurity Task Force to "engage state water sectors and water government coordinating councils in an effort to reduce risks of cyberattacks to nationwide water systems."

Further, in November 2024, the EPA Office of Inspector General (IG) issued a management implication report on cybersecurity concerns in drinking water systems (DWS).[30] The IG highlighted that 97 DWS serving approximately 26.6 million users have either critical or high-risk cybersecurity vulnerabilities. Additionally, 211 DWS, servicing over 82.7 million people, had medium and low vulnerability scores. The IG stressed that cybersecurity risks exist for all facilities within DWS.

Additionally, the White House and EPA further pressed states to act independently. In a letter to the States in March 2024, highlighting that "the National Security Council (NSC) and EPA are encouraging all states to join this dialogue to drive rapid improvements to water cybersecurity and reinforce collaboration between state and federal entities and water systems."[31]

Until comprehensive federal regulations to address cybersecurity in the WWS sector are enacted, it will continue to be incumbent on states to secure their water systems. As of late 2024, various states have begun to take action, and some of these actions are discussed further in the Recommendations section below.

1.4 Challenges to Increase Security

On March 11, 2024, the White House met with States following the joint EPA-White House letter.[32] One of the common themes that emerged was the need for additional financial resources to improve security. State leaders noted the need for funding; many times, the first roadblock highlighted to improving security is financial. Separately, research has also identified

---

[30] U.S. EPA Office of Inspector General, "Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems," November 13, 2024, https://www.epaoig.gov/reports/other/management-implication-report-cybersecurity-concerns-related-drinking-water-systems.

[31] US EPA, "Biden-Harris Administration Engages States on Safeguarding Water Sector Infrastructure against Cyber Threats," News Release, March 19, 2024, https://www.epa.gov/newsreleases/biden-harris-administration-engages-states-safeguarding-water-sector-infrastructure.

[32] U.S. EPA, "Biden-Harris Administration Engages States on Safeguarding Water Sector Infrastructure against Cyber Threats," News Release, March 19, 2024, https://www.epa.gov/newsreleases/biden-harris-administration-engages-states-safeguarding-water-sector-infrastructure.

a lack of sufficient funds as the most significant barrier.[33] Additionally, the need for additional cybersecurity experts is often highlighted across the spectrum of cybersecurity. Qualified staffing is further complicated in industrial cybersecurity due to the lack of people understanding OT and IT.

The World Economic Forum (WEF) reported in their *Global Cybersecurity Outlook 2025* report that smaller organizations struggle to ensure cyber resilience.[34] Additionally, 71% of cyber leaders believe "small organizations have already reached a critical tipping point where they can no longer adequately secure themselves against the growing complexity of cyber risks." In the absence of funding and qualified staff, the WEF highlighted that "cybersecurity training and awareness initiatives are vital parts of an effective risk management strategy."[35] The WEF cited the 2024 Cybersecurity Skills Gap global research report, which noted three key factors that hinder cybersecurity.[36] These factors are:

1. An IT/security staff that lacks the necessary skills and training
2. A lack of organizational or employee security awareness
3. A lack of cybersecurity products

While portions of these items may be costly to implement and require additional financial resources, many cybersecurity training and awareness resources are available to State and Local governments at low to no cost. Training through CISA and the EPA or partnering with organizations such as those highlighted in the Recommendations section can effectivily improve cybersecurity without requiring great financial investment.

> "While central governments and national agencies often receive substantial attention in cybersecurity dialogues, local governments stand uniquely vulnerable due to a limited budget, a lack of cybersecurity infrastructure and expert workforce, the absence of regulatory compliance, and a lack of prioritization by the concerned authorities."[37]

Further, the cost of preventing a cyber attack is lower than the cost of remediating a cyber attack, not to mention the potential damage to public trust in an organization when those they rely on suffer a cyber incident. Therefore, conducting cybersecurity awareness and training at all portions of the WWS sector is important. Training water plant staff and those responsible for budgets and IT/OT. Increased cybersecurity awareness and training will positively affect the

---

[33] Sk Tahsin Hossain et al., "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework," *Applied Sciences* 14, no. 13 (June 25, 2024): 5501, https://doi.org/10.3390/app14135501.

[34] World Economic Forum. "Global Cybersecurity Outlook 2025." Insight Report. Geneva, Switzerland, January 13, 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[35] Rob Rashotte, "3 Key Factors to Make Your Cybersecurity Training a Success," October 30, 2024, https://www.weforum.org/stories/2024/10/3-key-factors-to-make-your-cybersecurity-training-a-success/.

[36] Fortinet Training Institute, "2024 Cybersecurity Skills Gap," June 20, 2024, https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf.

[37] Sk Tahsin Hossain et al., "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework," *Applied Sciences* 14, no. 13 (June 25, 2024): 5501, https://doi.org/10.3390/app14135501.

security of the Maryland WWS sector. Organizations should take a human-centered cybersecurity (HCC) approach, which "involves the social, organizational, and technological influences on people's understanding of and interactions with cybersecurity."[38]

1.5 Additional Opportunity for Maryland Cyber Leadership

Maryland has worked to improve cybersecurity in the WWS sector, as noted by the efforts of the Modernize Maryland Act of 2022 and through efforts within the MDE, DoIT, and MDEM. Following the 2024 Letter to the States, MDE has led the formation of a state plan to increase cybersecurity in the WWS sector and submitted it to the White House as required. These collaborative efforts are positive steps to improve cybersecurity in the sector and address the EPA's current guidance that states work to secure their WWS sector and reduce cyber risk.

Until greater funding is available or programs increase qualified cybersecurity staff, the strongest recommendations are to increase cybersecurity awareness and training with the Maryland WWS sector and those responsible for oversight and governance of the facility. While budgets are a limited resource, investments into cybersecurity where they can be made will help prevent costly incidents. With free to low-cost training and collaboration across the state, there are opportunities to secure the sector without significantly increasing the financial burden on water plants.

> "Together, we're going to have to change how we do things. As our community innovates, it must also build the defences and through those defences our resilience. We have to make sure that technology is working for us as consumers, as users, as people..." -- UK NCSC CEO Dr Richard Horne[39]

2. RECOMMENDATIONS

The recommendations of this report seek to identify additional opportunities for the State of Maryland to increase cybersecurity at all levels. Recommendations aim to provide a holistic approach to security, from regulation and oversight to training and awareness. Additionally, the research for this report began in February 2024, and since that time, Departments have already taken steps to improve security, and those efforts are recognized in the recommendations. This report's recommendations include further strengthening some of these efforts with legislative action.

---

[38] Jody Jacobs and Julie Haney, "Learning, Sharing, and Exploring with NIST's New Human-Centered Cybersecurity Community of Interest," *NIST*, September 4, 2024, https://www.nist.gov/blogs/cybersecurity-insights/learning-sharing-and-exploring-nists-new-human-centered-cybersecurity.

[39] Horne, Dr. Richard. "NCSC CEO's Speech to Mark the Launch of the NCSC Annual Review 2024." Speech, December 3, 2024. https://www.ncsc.gov.uk/speech/ncsc-annual-review-launch-2024-ceo-dr-richard-horne.

2.1 Governance and Policy

2.1.1 Regulatory Goals

Several entities at the State and Federal levels regulate the WWS sector in Maryland.[40] First, the MDE is the State's primacy agency under the SDWA Amendments of 1996. It administers the State's Operator Certification Program through the MDE Water Supply Program. The SDWA regulates systems that provide water to 25 or more individuals, and a public water system is one serving water to 25 or more individuals a day for more than 60 days per year.

> The EPA defines a public water system (PWS) as "a public water system provides water for human consumption through pipes or other constructed conveyances to at least 15 service connections or serves an average of at least 25 people for at least 60 days a year. A public water system may be publicly or privately owned."

At the Federal level, Presidential Policy Directive (PPD) 21 and Executive Order 13636 designated the EPA as the Sector Risk Management Agencies (SRMA) for the WWS sector. Each SRMA is selected based on its institutional knowledge and specialized expertise in that sector. As the SRMA, they "coordinate with DHS and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT[41] entities, as appropriate to implement PPD-21," and "provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate."

In March 2024, the White House initiated a requirement for each state to produce a Water Sector Cybersecurity Plan. The MDE Water Supply Program Manager and team led the effort to develop the plan. They will be leading the effort to implement it. Formalizing the MDE as the Maryland sector lead would create a known sector lead for those needing to reach out and engage the WWS sector. Within the Maryland WWS sector, MDE is a trusted agent to help facilities, and it "speaks the language" of the sector, able to help translate between water systems and cybersecurity-focused entities. While the Maryland Department of Information Technology (DoIT), Office of Security Management (OSM), led by the State CISO, is responsible for cybersecurity policy, MDE would help implement efforts within the WWS sector. MDE would not assume leading cybersecurity policy efforts because of its designation as the State Sector Lead for water security.

> **RECOMMENDATION 1**: Officially designate the MDE as the lead agency for coordinating security efforts within the Maryland WWS sector. Additionally, MDE should coordinate with other State agencies regarding cybersecurity policies and efforts targeting the WWS sector.

According to the MDE, over 2,000 certified water treatment plant operators in Maryland oversee the treatment and distribution of safe drinking water. MDE has the authority to include a cybersecurity section as part of the operator certification process. Including cybersecurity

---

[40] Maryland MDE, "Laws and Regulations Governing the MDE Water Supply Program," accessed November 12, 2024, https://mde.maryland.gov/programs/water/water_supply/Pages/default.aspx.
[41] State, local, tribal, and territorial (SLTT) governments

basics in the operator and superintendent certifications would bring awareness of cybersecurity to those individuals operating water plants. Further, as cybersecurity is an evolving topic, including continuing education requirements for those renewing their certifications would help ensure they are made aware of changing cybersecurity practices.

As part of the Maryland plan, the MDE Water Supply Program will add a cybersecurity awareness component to the operator certification program under its existing authorities. MDE will utilize EPA water sector-specific training for those seeking to maintain certification. Successful completion of the EPA awareness training will be provided to MDE during certification renewal every three years.

> **RECOMMENDATION 2**: The State of Maryland should affirm support for the MDE plan to include the cybersecurity awareness component for all new and renewing operator and superintendent certifications.

As WWS sector facilities upgrade with modern OT and IT technologies and these systems converge[42], cybersecurity considerations must occur in the earliest design and implementation stages. A cybersecurity component should be added to the Maryland Minimum Design Standards to achieve the goal of integrating cybersecurity into the water systems.

> **RECOMMENDATION 3**: Amend Code of Maryland Regulations (COMAR) Quality of Drinking Water in Maryland, 26.26.04.01, to include a comprehensive section regarding cybersecurity standards for water and wastewater treatment facilities.[43]

In March 2023, the EPA sought to improve PWS cybersecurity by requiring states to survey cybersecurity during their sanitary surveys, specifically focused on OT used for safe drinking water. The EPA issued an interpretive memorandum titled "*Addressing Public Water System Cybersecurity in Sanitary Surveys of an Alternate Process*" to achieve the goal. Following a legal challenge by the State of Missouri, State of Missouri *v.* EPA (23-1787), the EPA rescinded the memorandum.

In August 2024, the U.S. GAO issued a report (GAO-24-106744) titled "Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems." The GAO highlighted the increased cyber risk to the water sector and noted that the "sector has made limited investments in cybersecurity protections because water systems prioritize funding to meet regulatory requirements for clean and safe water, while improving cybersecurity is voluntary." As part of the EPA response to the GAO, the EPA advised that they would be releasing a risk assessment and strategy for the water sector in January 2025.

While the EPA works to secure the sector, states have continued identifying opportunities to increase cybersecurity under their authority. In one example, the Governor of Minnesota signed

---

[42] Stephen J. Bigelow, "What Is IT/OT Convergence? Everything You Need to Know," Search IT Operations, https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence.
[43] Chapter 01 Quality of Drinking Water in Maryland
https://mde.maryland.gov/programs/regulations/water/Documents/26.04.01.01%2C%20.01-1%2C%20.20%2C%20and%20.37.pdf

Executive Order 22-20, Directing State Agencies to Implement Cybersecurity Measures to Protect Critical Infrastructure in Minnesota.[44] To comply with the EO, the Minnesota Department of Health (MDH), under its Drinking Water Protection Program, required "all community Public Water Systems (PWSs) in Minnesota that utilize Operational Technology (OT), such as Supervisory Control and Data Acquisition (SCADA), must conduct an annual cybersecurity assessment and certify the completion with MDH."

In 2022, Maryland enacted House Bill 1205, the Modernize Maryland Act of 2022.[45] This Act required public or private water and wastewater systems that serve 10,000 or more users and receive financial assistance from the state to "(1) assess its vulnerability to a cyberattack; (2), if appropriate, develop a cybersecurity plan; and (3) submit a report to the General Assembly on the findings of the assessment and any recommendations for statutory changes needed for the system to appropriately address its cybersecurity" by December 1, 2023.

To strengthen the cybersecurity of the Maryland WWS sector, additional consideration should be given to systems with less than 10,000 users, as well as those not receiving financial assistance from the state. The assessment methodology in the Act, allowing for self-assessment, should be utilized in further legislation.

> **RECOMMENDATION 4**: Supplement the Modernize Maryland Act of 2022 with a new Act to address cybersecurity vulnerabilities in the greater Maryland WWS sector. Modeling after the Minnesota EO, require PWSs in the state that use OT to conduct an annual cybersecurity assessment and certify compliance with the MDE.

2.1.2 The Need for a National Strategy

Worldwide, the importance of critical infrastructure (CI) and its protection have led to an increase in regulations targeting CI protection. The European Union (EU) specifically noted that its directive was because of "the growing threats posed with digitalisation and the surge in cyber-attacks."

> Examples of laws focused on CI protection:
>
> **EU:** Network and Information Security (NIS2) Directive. The NIS2 focuses on sectors of high criticality, including drinking water and wastewater systems, equivalent to the U.S. WWS sector.
>
> **UK:** In September 2024, the UK announced it would introduce a Cyber Security and Resilience Bill in 2025 that will "strengthen the UK's cyber defences and ensure critical infrastructure and the digital services companies rely on are secure."

---

[44] Minnesota IT Services, "Executive Order 22-20 Summary," n.d., https://mn.gov/mnit/government/policies/security/eo22-20.jsp#:~:text=Executive%20Order%2022-20%20requires,across%20the%20State%20of%20Minnesota

[45] Maryland General Assembly, "Legislation - HB1205," State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022), July 8, 2022, https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb1205?ys=2022RS.

Singapore: The Cybersecurity (Amendment) Act 2024 strengthened cybersecurity for critical information infrastructure, which includes the water sector.

Hong Kong: Proposed new legislation in 2024 to "strengthen the security of the computer systems of critical infrastructure and minimise the chance of essential services being disrupted or compromised due to cyberattacks, thereby enhancing the overall computer system security in Hong Kong."

The EPA announced its plan to introduce a new water sector risk assessment and management plan in January 2025. Additionally, H.R. 7922, the Water Risk and Resilience Organization (WRRO) Establishment Act, was introduced in April 2024 to "establish a new governing body, the WRRO, with cyber and water-system expertise to develop and enforce cybersecurity requirements for drinking and wastewater systems."[46] While experts present issues with the WRRO approach, state governments should support the goal of strengthening cybersecurity in the WWS sector in some form. The WRRO would focus on WWS sector systems of 3,300 customers or more. While this increases security, it still leaves those smaller systems out of the requirement.

RECOMMENDATION 5: The State of Maryland should formally express its support for developing and implementing a robust national cybersecurity policy covering the entirety of the WWS sector. The plan should be tailored to the specific needs of the WWS sector, and support should highlight the benefits of a national strategy to reduce cyber risk instead of requiring states to work independently.

2.1.2 Artificial Intelligence

Artificial Intelligence (AI) offers increased opportunities to help protect Maryland's critical infrastructure, especially the WWS sector. The U.S. Department of Homeland Security (DHS) uses the AI Safety and Security Board (AISSB) to provide "recommendations to prevent and prepare for AI-related disruptions to critical services that impact national or economic security, public health, or safety." DHS also created "Safety and Security Guidelines for Critical Infrastructure Owners and Operators" with three guiding principles for operators: Map, Measure, and Manage.

At the same time, cyber threat actors also leverage AI to increase their attacks. DHS warned CI operators of increased threats due to AI's use. In October 2024, OpenAI, the company behind ChatGPT, issued a report detailing the CyberAv3ngers group utilizing AI for reconnaissance, target intelligence and vulnerabilities, and debugging malicious code.[47] The group also used AI to identify default usernames and passwords for Programmable Logic Controllers (PLCs) used within critical infrastructure.

---

[46] 118th Congress, "H.R.7922 - To Establish a Water Risk and Resilience Organization to Develop Risk and Resilience Requirements for the Water Sector," April 10, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7922.

[47] OpenAI, "Influence and Cyber Operations: An Update," October 2024, https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf.

Specific to Maryland, in 2024, Governor Moore issued Executive Order 01.01.2024.02, creating the AI Subcabinet, authorized by statute in Chapter 496, Acts of 2024.[48] A goal of the Subcabinet is to create recommendations for critical domains.

> **RECOMMENDATION 6**: Recommend that the AI Subcabinet, in coordination with Maryland DoIT and the MCC Critical Infrastructure Subcommittee, examine AI's impact on Maryland CI, including the WWS sector. Recommend providing guidance for the sector to utilize AI and defend against AI-enabled threats.

2.1.3 Cybersecurity Reporting and Transparency

Reporting cybersecurity incidents is important to aid the understanding of what is happening in the WWS sector regarding cyber incidents. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires covered entities to "report to CISA any covered cyber incidents within 72 hours from the time the entity reasonably believes the incident occurred."[49] In Maryland, covered entities include Community Water Systems (CWSs), which serve more than 3,300 people, and wastewater treatment facilities. Smaller systems are not required to report under CIRCIA; however, information about cyber incidents involving these systems is still an important data point.

> "Every victim of a cyber incident should report it to CISA, every time, recognizing that **a threat to one is a threat to many**, because cybersecurity is national security."[50]
>
> -- Jen Easterly, former Director, CISA

In discussion with the Maryland CISO the importance of timely reporting to be able to leverage cybersecurity information in a tactical manner was highlighted. Therefore, rather than waiting up to 72 hours to report an incident, faster reporting would help Maryland better react to a cyber incident and assist the WWS facility in need. The Maryland CISO recommended that incident reporting happen within 24 hours.

To better understand the cyber threat against the Maryland WWS sector, help inform the sector, and provide better protection against threats, Maryland should encourage all WWS sector members to report cyber incidents. Filing reports of incidents with the State of Maryland, CISA, and the FBI all help inform the security community about ongoing cyber threats. Hosted by the FBI, "the Internet Crime Complaint Center (IC3) is the central hub for reporting cyber-enabled crime."

---

[48] Governor Wes Moore, "EXECUTIVE ORDER 01.01.2024.02 Catalyzing the Responsible and Productive Use of Artificial Intelligence in Maryland State Government," January 8, 2024, https://governor.maryland.gov/Lists/ExecutiveOrders/Attachments/31/EO%2001.01.2024.02%20Catalyzing%20the%20Responsible%20and%20Productive%20Use%20of%20Artificial%20Intelligence%20in%20Maryland%20State%20Government_Accessible.pdf.

[49] US CISA, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," accessed November 12, 2024, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

[50] Easterly, Jen. "Strengthening America's Resilience Against the PRC Cyber Threats," January 15, 2025. https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats.

> **RECOMMENDATION 7**: Amend Code of Md. Regs. Quality of Drinking Water in Maryland. 26, § 26.04.01.19, Reporting Requirements, to include a requirement that a supplier of water report cyber incidents within 24 hours.

Further, employees within a WWS sector facility must understand the need to report suspicious activity as soon as possible. Beyond stressing the importance, facilities should implement a cyber incident reporting program that clearly explains what information to report. Additionally, a module regarding incident reporting procedures should be included in employee annual training. Stress to employees that there is no retaliation for reporting suspected incidents. It is better to report and find that the activity was authorized than to miss an opportunity to stop an attack. Proactive reporting will help to minimize potential damage and downtime.

> **RECOMMENDATION 8**: Recommend WWS sector facilities create and maintain a robust cyber incident reporting program and include the program in annual security training.

How will the State respond if there is a major incident that requires water service to be supplemented?

Regardless of whether a WWS sector facility is public or private, those responsible for its operation should prepare a Cybersecurity Incident Response Plan in case a cyber attack happens against their water system. Should a cyber incident occur, it is important to communicate information to residents and customers of the system and ensure they are aware of the steps taken to mitigate disruptions to the system. Through late 2024, most attacks against the U.S. WWS sector have seen minimal water treatment and distribution disruption. They are often more disruptive against the IT system, especially billing. Minimal impact may not always be the case, as demonstrated in Ireland in December 2023, where a town was without water for two days following a cyber attack against their OT system.[51]

In October 2024, American Water, the largest publicly owned water and wastewater utility company in the U.S., issued a notice that they had a cyber incident involving unauthorized access to their systems. American Water noted that they disconnected or deactivated systems to protect customer data; however, there was no impact on water and wastewater services. American Water provided this information via a webpage and through the media. American Water operates in Maryland through its subsidiary, Maryland American Water, serving approximately 23,000 people.

Highlighting the importance of Crisis and Emergency Risk Communication (CERC), the California Division of Drinking Water (DDW) collaborated to create a Crisis and Emergency Risk Communication Tool Kit for community water systems.[52] This tool kit helps facilities "effectively

---

[51] "Two-Day Water Outage in Remote Irish Region Caused by pro-Iran Hackers." Accessed January 28, 2025. https://therecord.media/water-outage-in-ireland-county-mayo.
[52] California State Water Resources Control Board, "Water Resiliency - Crisis and Emergency Risk Communication (CERC)," https://www.waterboards.ca.gov/drinking_water/certlic/drinkingwater/water_resiliency/prepare.html#cerc.

manage and communicate during an emergency or crisis." California used grant funding from the U.S. EPA and CDC.

> **RECOMMENDATION 9**: Allocate funding, or seek grants, to enable the Maryland Department of Emergency Management (MDEM) to create a cyber-focused CERC plan for Maryland, especially the WWS sector. Alternatively, consider leveraging the California plan.

Additionally, to help Maryland residents prepare should a major cyber attack impact their water services, provide information through the MDEM MD Ready website. The MD Ready Alert system could also be leveraged to notify customers should mass communication be required.

> **RECOMMENDATION 10**: Include cybersecurity attack information on the MDEM "Know the Threats" website and consider the MD Ready as an alerting system if required.

To best connect cybersecurity resources with the appropriate person, each facility in the Maryland WWS sector should appoint an individual as the primary point of contact for cybersecurity. This individual should understand the operation of the WWS facility and the ICS/OT. While this person may not be the primary IT person for the facility, they can act as a liaison between the different parts of the local WWS and a conduit to receive information from the State as required. A readily identified point of contact (POC) could be especially important if information were to become known that a particular facility was at risk. The primary POC would reduce the time it may take to disseminate information.

> **RECOMMENDATION 11**: MDE should encourage/require each WWS sector facility, or managing government or office, to appoint a primary point of contact for cybersecurity.

2.1.4 Privacy

Information about specific infrastructure and cybersecurity within a WWS sector facility is sensitive information that should be protected from public disclosure. This information can detail specific vulnerabilities and provide threat actors with key information for attack planning. Therefore, the protection of this information is in the interest of security.

Several U.S. states have taken steps to protect information voluntarily submitted to the state.

- Ohio: In 2022, Amended Section 149.433 | Exempting security and infrastructure records. Records are protected from disclosure related to security or infrastructure that is provided to the state outside of required public notifications.
- Texas: Exempts confidential network security information from public disclosure under Texas Government Code 552 (Public Information Act).

Maryland General Provisions Code § 4-338 protects information systems, directing "a custodian shall deny inspection of the part of a public record that contains information about the security of an information system." To further protect sensitive information regarding a CI system, expand the wording of this exemption.

> **RECOMMENDATION 12:** The State of Maryland should amend its Public Information Act (PIA) § 4-338 to explicitly exempt sensitive security and infrastructure information

voluntarily provided to state agencies. Recommend expanded wording which notes, "a custodian shall deny inspection of the part of a public record that contains information about the security of an information system or critical infrastructure system."

Smart water meters are being installed in customer locations to increase the efficiency of billing and water management; however, they also create a potential privacy risk for customers. In addition to collecting water use data, truly smart meters can control water service through remote turn on or shut off and alert the utility to water issues such as high flow, reverse flow, low or high pressure, and other issues. Further, one smart meter manufacturer notes that hourly customer data is logged for 120 days.[53]

As utilities, or the entity responsible for managing their billing, hold personal information about Maryland residents, it is imperative that this information is protected from unauthorized access and disclosure. To protect residents, States have passed legislation providing greater protection to residents and implementing data breach notification procedures required of those who hold the data.

Nevada: 2023 Nevada Revised Statutes Chapter 603A - Security and Privacy of Personal Information. Under this law, Nevada utilities must keep customer information confidential and abide by its requirements.

Colorado: Colorado Privacy Act Rules, 4 CCR 904-3, protects residents' data and, "The law applies to entities, including nonprofits, that conduct business in Colorado or deliver commercial products or services targeted to residents of Colorado; AND either:

Process the personal data of more than 100,000 individuals in any calendar year; or

Derive revenue or receive discounts on goods or services in exchange for the sale of personal data of 25,000 or more individuals."[54]

Texas: State law gives consumers ownership of the data generated and collected by smart meters and provides consumer protection as utilities are only allowed to use the data for billing purposes.

On the website of the Maryland Office of People's Counsel (OPC), they address Maryland resident privacy concerns regarding smart meters[55]:

"Customers have expressed concern about their privacy and controlling who has access to their usage information. Utilities cannot release customer data to third parties without your permission, unless required by a warrant or subpoena. Advanced Meter Infrastructure ("AMI") meters, otherwise known as smart meters,

---

[53] Xylem, "Smart Water," accessed November 13, 2024, https://www.xylem.com/en-us/solutions/smart-utility-networks/smart-water/.
[54] Colorado Attorney General, "Colorado Privacy Act (CPA)," accessed November 13, 2024, https://coag.gov/resources/colorado-privacy-act/.
[55] Maryland Office of People's Counsel, "Smart Meters," n.d., https://opc.maryland.gov/Consumer-Learning/Electricity/Smart-Meters.

do not change that utility obligation. OPC supports strong customer privacy rules and will continue to monitor and remain engaged with the utilities and the PSC over privacy and cybersecurity concerns related to AMI meters."

RECOMMENDATION 13: Maryland should consider enacting a privacy act focusing on smart meters and utilities and informing residents about their options to protect their privacy.

Operator Privacy

The certified water operator and superintendent databases help confirm certifications and potentially locate additional staff. However, at the same time, having a central database disclosing the names and information of the certified operators also creates a potential vulnerability. As noted earlier, with business email compromise and phishing schemes regularly utilized by threat actors, it is worthwhile to consider protecting these lists.

The Vermont Department of Environmental Conservation, Drinking Water and Groundwater Protection Division has created a Drinking Water Database Search that is not password protected but requires the user to enter a portion of the name or operator ID to obtain information. Example: https://anrweb.vt.gov/DEC/DWGWP/

RECOMMENDATION 14: MDE should implement measures to protect the "List of Active Certified Operators" maintained on its website while ensuring legitimate access for necessary purposes.

2.2 Foundational Cybersecurity

2.2.1 Cyber Hygiene and Best Practices

Cyber hygiene refers to the basic practices and precautions individuals and organizations take to maintain the security and health of their digital systems and data. In many instances, these best practices can be low to no cost, less complex, and less complicated to implement and the practices increase the security of the WWS sector. The criticality of these practices was noted by Director of National Intelligence Avril D. Haines in a presentation on May 2, 2024, noting:

"In virtually all the attacks we've seen against U.S. critical infrastructure, cyber actors took advantage of default or weak passwords; unpatched, known vulnerabilities; and poorly secured network connections to launch relatively simple attacks. And for this reason, it is crucial that all of us — particularly critical infrastructure owners and operators — improve our cybersecurity practices to reduce our vulnerability to such efforts." [56]

Demonstrating the need for even rudimentary cybersecurity measures were the 2024 state-affiliated actors from China Salt Typhoon hacks against U.S. telecommunications companies. Even though this is a different critical infrastructure sector, people would typically believe that

---

[56] C. Todd Lopez, "Good Cyber Hygiene Can Impede Adversary Meddling in U.S. Infrastructure," DOD News, May 2, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3763862/good-cyber-hygiene-can-impede-adversary-meddling-in-us-infrastructure/.

better-resourced major telco companies would have implemented even the best basic cyber practices. However, the White House reported the failure of the companies to implement rudimentary cybersecurity measures within their IT infrastructure.[57] The capabilities of Salt Typhoon demonstrate the capabilities of Chinese cyber actors at large, targeting critical U.S. infrastructure, including the Volt Typhoon group. These attacks further demonstrated the need to implement basic cyber practices within the WWS sector.

Therefore, it is important that the Maryland WWS sector increase basic cyber hygiene within the facilities and networks. The Center for Internet Security (CIS) offers CIS Critical Security Controls®, which include measures to help achieve essential hygiene. CISA also offers "Cybersecurity Best Practices for Industrial Control Systems."[58]

> **RECOMMENDATION 15**: MDE, in partnership with DoIT, should recommend that the WWS sector adopt basic cyber hygiene practices, such as those outlined in CIS Critical Security Controls, to help address security gaps and strengthen the sector.

2.2.1.1 Passwords and Credentials

Stopping a threat actor "at the door" is an important part of cybersecurity, and it is especially important to continue to challenge a user's identity as they move throughout the WWS IT or OT network. Unique user IDs, strong passwords, multi-factor authentication (MFA), granting users the least privilege required, and regular review of user credentials are important steps that a system can take to help secure the network. When an employee or person with access to a system no longer requires access or leaves the organization, their credentials should be revoked or canceled immediately. Additionally, systems should change default user IDs and passwords for ICS infrastructure and devices, such as PLCs (Programmable Logic Controllers), VFDs (Variable-Frequency Drives), and HMIs (Human-Machine Interfaces).

Passwords are one of the weakest links in security.[59] According to the Verizon 2024 Data Breach Investigations Report, brute force attacks, usually against weak passwords, accounted for 21% of the top hacking actions in web application attacks.[60] In August 2024, NIST released an updated draft of Special Publication 800-63, *Digital Identity Guidelines,* providing updated password guidance and recommendations.[61] The updated NIST guidance focuses on password

[57] Otto, Greg. "White House: Salt Typhoon Hacks Possible Because Telecoms Lacked Basic Security Measures." CyberScoop, December 27, 2024. https://cyberscoop.com/salt-typhoon-telecom-cybersecurity-gaps-white-house-response/.

[58] U.S. CISA, "Cybersecurity Best Practices for Industrial Control Systems," December 17, 2020, https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-industrial-control-systems.

[59] Chris Smith, "Millions of People Replaced Passwords with Passkeys, so Why Haven't You?," *BGR* (blog), November 21, 2024, https://bgr.com/tech/millions-of-people-replaced-passwords-with-passkeys-so-why-havent-you/.

[60] Verizon Business, "2024 Data Breach Investigations Report," May 1, 2024, http://verizon.com/dbir.

[61] David Temoshok et al., "Digital Identity Guidelines: Authentication and Authenticator Management" (Gaithersburg, MD: National Institute of Standards and Technology, 2024), https://doi.org/10.6028/NIST.SP.800-63B-4.2pd.

length rather than complexity and forced changes.[62] For Maryland WWSs, it is important that they regularly perform password management and integrate NIST recommendations. Additionally, implementation of MFA, which requires two or more authenticators, makes accounts "99% less likely to be hacked," according to CISA, and the UK's National Cyber Security Centre (NCSC) stresses that implementation of any MFA is superior to a password alone.[63][64] Further, it is recommended that organizations use phishing-resistant MFA.[65]

Regarding user credentials, NIST SP 800-82r3 provides guidance on Identity Management and Access Control and highlights the "life cycle for managing OT credentials, including issuance, revocation, and updates across the OT environment." Strong credential management can help prevent unauthorized access and protect against insider threats.

2.2.1.2 Network Segmentation

Protecting the IT/OT boundary is important, especially as the convergence of the two networks has reduced traditional separation. Addressing the ASCS principle of network segmentation, several cyberattacks in 2024 against the WWS sector have highlighted the importance of OT and IT network segmentation. In one of the most recent incidents, New Jersey-based American Water, the largest regulated water and wastewater utility company in the U.S., announced on October 7 that it had been the victim of a cyberattack. American Water had to shut down some of its systems to protect customer data, including billing. Without proper network segmentation, once a malicious cyber actor has gained access to the network, they can move to other portions of the network, which could cause physical damage if they move into the OT network. If maintaining separate networks is no longer possible, it is important to ensure that strong protections are in place.

2.2.1.3 Air-gap

One strategy to maintain network segmentation is to physically and logically separate the sensitive network from other networks and the internet via the air-gap technique, where the network's isolation seeks to protect sensitive assets and information. This method can reduce cyber threats when correctly implemented, given the lack of direct online access to the network. However, air-gapped networks can still face cyberattacks, especially against well-resourced adversaries. Research by Guri (2024) provided details of vulnerabilities and attacks

---

[62] Edge Editors, "NIST Drops Password Complexity, Mandatory Reset Rules," Dark Reading, September 25, 2024, https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules.

[63] U.S. CISA, "Multifactor Authentication," https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication.

[64] UK National Cyber Security Centre, "Why MFA Matters," September 26, 2024, https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/why-mfa-matters.

[65] U.S. CISA, "Implementing Phishing-Resistant MFA," 2022, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

against air-gapped networks, demonstrating that this method alone is not entirely secure.[66] However, air-gap can be a strong security measure in the WWS sector.

> **RECOMMENDATION 16**: MDE, in partnership with DoIT, should encourage the WWS sector to adopt best practices, including password and identity management, and network segmentation. WWS systems should also ensure that they reduce cyber vulnerabilities.

CISA has prepared a fact sheet providing cyber actions the WWS sector can take to improve security within their facilities.[67] The fact sheet provides links to free services, resources, and tools.

> **RECOMMENDATION 17**: Ensure WWS sector facilities are aware of the "Top Cyber Actions for Securing Water Systems" fact sheet and help direct them to additional resources as needed.

> **RECOMMENDATION 18:** MDE, in collaboration with the Maryland Cybersecurity Coordinating Council (MCCC), should actively promote and support the implementation of CISA's "Top Cyber Actions for Securing Water Systems" fact sheet by all Water and Wastewater Systems (WWS) in Maryland.

2.2.1.4 Zero Trust and Secure by Design

Zero Trust

"Zero Trust (ZT) is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries." The ZT security model assumes that a breach is inevitable or has likely already occurred and utilizes the concept of least-privileged access to be applied for every access decision.[68]

The guiding principles for ZT are:

- **"Never trust, always verify** – Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
- **Assume breach** – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.

---

[66] Mordechai Guri, "Mind The Gap: Can Air-Gaps Keep Your Private Data Secure?" (arXiv, 2024), https://doi.org/10.48550/ARXIV.2409.04190.

[67] U.S. CISA, "Top Cyber Actions for Securing Water Systems," February 23, 2024, https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems.

[68] Scott Rose et al., "Zero Trust Architecture" (National Institute of Standards and Technology, August 11, 2020), https://doi.org/10.6028/NIST.SP.800-207.

- **Verify explicitly** – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources."

Zero Trust is a security model that the WWS sector and their associated governments or companies can choose to implement. One of the key items is that those responsible for the IT and OT infrastructure operation must agree to implement the model and its associated architecture.

Additionally, while ZT is a complex security concept with many different facets and takes time and resources to implement, it is important that WWS organizations adopt the concept and begin taking steps to implement ZT in their architecture. CISA highlights in their Zero Trust Maturity Model (ZTMM) Version 2.0 that "the path to zero trust is an incremental process that may take years to implement."[69] CISA also describes ZT maturity as a journey that evolves from the traditional enterprise architecture towards the optimal ZT architecture. CISA notes a shortcoming of the ZTMM is that it does not address challenges specific to OT; however, resources are available specific to ZT implementation in OT environments. Organizations may need to use multiple resources to secure IT and OT systems.

> **RECOMMENDATION 19**: Recommend WWS entities and those responsible for their IT and OT adopt a ZT security model and leverage the ZT materials provided by the U.S. government as free resources.

Secure by Design

Secure by Design principles, according to CISA, "prioritize the security of customers as a core business requirement, rather than merely treating it as a technical feature." The goal of Secure by Design is to shift the cybersecurity burden from the consumers and organizations that use a product back towards the producers of the products and technologies that are digital and connected. While this will not remove all cybersecurity burdens from the end users, it will help users as products are designed with security in mind rather than as an afterthought. While this differs from ZT, where the users can decide to adopt the model, with Secure by Design, it is on the producers to decide to adopt this practice. It is worth noting that the education of the WWS sector about product security can aid when choosing a new product or technology to adopt, asking the provider about the device's security, and implementing security.

> **RECOMMENDATION 20**: Through DoIT's cybersecurity portal, improve awareness of Secure by Design features among Maryland State and Local Government officials and private water companies. MDE should encourage WWS sector facilities to select upgraded equipment that meets Secure by Design principles when available.

The National Security Agency (NSA) and its partners released a Cybersecurity Information Sheet (CSI) titled "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators in the Selection of Digital Products" in January 2025, providing key security elements

---

[69] Cybersecurity Division, U.S. CISA. "Zero Trust Maturity Model," 2023.

that should be considered when purchasing ICS and OT products.[70] The CSI details 12 elements that should be considered and provides strong guidance for purchasing decisions.

2.2.2 Adopting Frameworks

Cybersecurity experts note that adopting a cybersecurity framework will help an organization improve cybersecurity. The 2023 Nationwide Cybersecurity Review (NCSR) found that organizations that have adopted a framework scored 60% higher when assessing their cybersecurity maturity than those that have not.[71] Released in 2024, the NIST Cybersecurity Framework (CSF) 2.0 helps those developing and leading cybersecurity programs manage risk regardless of size or sector. Through its Cybersecurity Framework website, NIST provides additional free resources organizations can use to adopt the CSF.

> **RECOMMENDATION 21**: MDE should recommend WWS organizations in Maryland implement NIST CSF 2.0 to improve cybersecurity. Adoption of a framework can help an organization reduce its cyber risk.

NIST Special Publication 800-82r3 provides guidance to secure OT while addressing the unique aspects of OT performance, reliability, and security.[72] This guidance can provide a helpful starting point for those seeking to improve the security of their OT.

> **RECOMMENDATION 22**: MDE should encourage the WWS sector in Maryland to follow NIST SP 800-82r3 and implement NIST's security recommendations.

There are many other standards and frameworks that the WWS sector could utilize. This list is not inclusive but demonstrates the variety of available sources.

- American Water Works Association (AWWA) G430-14(R20) Security Practices for Operation and Management – "standard covers the minimum requirements for a protective security program for a water, wastewater, or reuse utility."
- ISO/IEC 27001 – "standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system."
- ISA/IEC 62443 series of standards – "set cybersecurity benchmarks in all industry sectors that use industrial automation and control systems (IACS)."

---

[70] U.S. CISA. "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators When Selecting Digital Products." U.S. National Security Agency, January 13, 2025. https://media.defense.gov/2025/Jan/13/2003626906/-1/-1/0/JOINT-GUIDE-SECURE-BY-DEMAND-PRIORITY-CONSIDERATIONS-OT-OWNERS-OPERATORS.PDF.

[71] The Center for Internet Security, Inc., and Multi-State Information Sharing and Analysis Center. "Nationwide Cybersecurity Review," December 10, 2024. https://www.cisecurity.org/insights/white-papers/nationwide-cybersecurity-review-2023-summary-report.

[72] Keith Stouffer et al., "Guide to Operational Technology (OT) Security" (Gaithersburg, MD: National Institute of Standards and Technology (U.S.), September 28, 2023), https://doi.org/10.6028/NIST.SP.800-82r3.

- Five ICS Cybersecurity Critical Controls – "sets forth the five most relevant critical controls for an ICS/OT cybersecurity strategy that can flex to an organization's risk model, and provides guidance for implementing them."

The Purdue Enterprise Reference Architecture, more widely referred to as the Purdue Model, was developed by Theodore Williams. It created levels within an ICS system and recommended ways to secure IT and OT networks as they interconnect. This framework was further adopted by the SANS Organization and modified into the ICS410 SCADA Reference Model.

> **RECOMMENDATION 23**:MDE should recommend that WWS organizations in Maryland adopt a reference model appropriate for their OT network to guide security improvements.

> **RECOMMENDATION 24:** MDE, in collaboration with the Maryland Cybersecurity Council (MCC) and DoIT, should develop and promote a guidance document that outlines recommended cybersecurity frameworks and standards for WWS in Maryland.

In October 2024, the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC), in partnership with CISA, other U.S. government agencies, and international partners, released the guide "Principles of Operational Technology Cybersecurity."[73] The guide provides six principles to create and maintain a safe, secure operational technology (OT) environment. CISA encourages critical infrastructure organizations to implement the recommendations to ensure proper cybersecurity controls are in place to help reduce risk to OT systems.

> The six principles are:
>
> 1. Safety is paramount
> 2. Knowledge of the business is crucial
> 3. OT data is extremely valuable and needs to be protected
> 4. Segment and segregate OT from all other networks
> 5. The supply chain must be secure
> 6. People are essential for OT cyber security

> **RECOMMENDATION 25:** Encourage the WWS sector members to become familiar with the six principles to ensure proper cybersecurity controls are in place. MDE and DoIT should partner to offer education and training regarding methods to implement these principles.

Organizations adopting cybersecurity frameworks and implementing best practices should assess their cybersecurity maturity regularly. One example option is the MS-ISAC and CIS Nationwide Cybersecurity Review (NCSR), a "no-cost, anonymous, annual self-assessment" available to local governments and their departments.[74] The NCSR provides the participants with metrics to identify gaps and benchmarks to assess year-to-year progress.

---

[73] U.S. CISA, "Principles of Operational Technology Cyber Security," October 1, 2024, https://www.cisa.gov/resources-tools/resources/principles-operational-technology-cyber-security.
[74] Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr

2.3 Risk Management and Resilience

2.3.1 Physical and Cyber Resilience Equal Water Resilience

"Organizational cyber resilience is the sum total of resiliency of all parts, which means that IT and OT can no longer be treated in isolation as holistic risk-management strategies are designed."

Global Cybersecurity Outlook 2025, The WEF

2.3.1.1 Physical Security

Cybersecurity does not stop with digital or connected systems. Physical security is an important component of cyber security, and CISA highlights that physical security best practices are crucial for cybersecurity. Access to the physical location of the IT and OT of the WWS facility can allow someone to introduce malware, make unauthorized changes, or even physically destroy equipment to impact WWS Sector operations. Even mistaken or inadvertent changes can impact system operation. To mitigate the risk to the infrastructure, WWS Sector facilities should ensure they have the best practices for physical security in place. "Protect the Physical Security of Your Digital Devices" training through CISA can help ensure physical security, and facilities should practice it.[75]

RECOMMENDATION 26: MDE should recommend that all Maryland WWS Sector facilities follow physical security best practices throughout their facility and remote locations. Additionally, systems should regularly review their physical security posture and make changes and improvements as necessary.

2.3.2 Emergency Response Planning

Through its Water Resilience efforts, EPA provides resources for emergency response planning, including cybersecurity.[76]

"Safe Drinking Water Act (SDWA) section 1433, which was amended by America's Water Infrastructure Act (AWIA) section 2013 in 2018, requires community water systems (CWS) serving more than 3,300 people to prepare or revise risk emergency response plans (ERPs) and certify to EPA that this work has been completed. SDWA section 1433(b) states that ERPs must "incorporate findings of the [risk and resilience] assessment' and "shall include strategies and resources to improve the resilience of the system, including...cybersecurity." The ERP must address the overall cybersecurity resilience of the water system and vulnerabilities found in the cybersecurity assessment portion of the RRA. A utility must incorporate the steps of preparing for, responding to, and recovering from a cyber incident in the ERP."

---

[75] U.S. CISA, "Protect the Physical Security of Your Digital Devices," https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices.
[76] US EPA, "Cybersecurity Planning," July 10, 2023, https://www.epa.gov/waterresilience/cybersecurity-planning.

RECOMMENDATION 27: MDE should expand the Emergency Response Plans (ERPs) requirement to include cybersecurity provisions for all community water systems (CWS).

2.4.1 Preparedness

It is imperative that WWS sector entities are prepared for a cyber incident. While much of the cybersecurity effort focuses on preventing attacks, organizations must include cyber recovery in their cyber resilience strategy. Cyber recovery, according to IBM, "is the process of increasing your organization's cyber resilience or ability to restore access to and functionality of critical IT systems and data in the event of a cyberattack."[77] Available from NIST, NIST SP 800-184 Guide for Cybersecurity Event Recovery helps organizations with comprehensive recovery planning.[78]

Further, the EPA has prepared an Incident Action Checklist – Cybersecurity for water utilities and provides copies via its Incident Action Checklists for Water Utilities website[79]. This checklist guides preparing, responding, and recovering from a cyber incident.

RECOMMENDATION 28: The MDE should actively promote adopting and utilizing the EPA's Incident Action Checklist – Cybersecurity by all WWS in Maryland.

CISA offers Cybersecurity Scenario CISA's Tabletop Exercise Packages (CTEPs) that are "cybersecurity-based threat vector scenarios including ransomware, insider threats, phishing, and Industrial Control System compromise."[80] These include CTEPs specifically tailored to WWS and ICS.

RECOMMENDATION 29: MDE, in partnership with MDEM and DoIT, should regularly host tabletop exercises tailored to the Maryland WWS sector to continue refining state and local government responses to cyber incidents.

The Maryland Department of Emergency Management's (MDEM) mission "is to proactively reduce disaster risks and reliably manage consequences through collaborative work with Maryland's communities and partners." MDEM creates and maintains the Maryland Consequence Management Operations Plan (CMOP), which outlines how "to prevent, prepare for, respond to, and recover from incidents affecting the lives of Marylanders." The CMOP maintains Critical Information Requirements (CIRs) focused on critical infrastructure, cybersecurity, and response.

RECOMMENDATION 30: As part of MDEM's planning, ensure that:

- Planning occurs specifically for cyber incidents impacting the WWS sector, especially those that may disrupt water service to Maryland residents and businesses.

---

[77] "Cyber Recovery vs. Disaster Recovery: What's the Difference? | IBM," July 17, 2024, https://www.ibm.com/think/topics/cyber-recovery-vs-disaster-recovery.

[78] Michael Bartock et al., "Guide for Cybersecurity Event Recovery" (Gaithersburg, MD: National Institute of Standards and Technology, 2016), https://doi.org/10.6028/NIST.SP.800-184.

[79] https://www.epa.gov/waterutilityresponse/incident-action-checklists-water-utilities

[80] U.S. CISA, "CISA Tabletop Exercise Packages," https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.

- Plans for alternative water supplies and mutual aid agreements should water services be unavailable, and the community require water needs to be delivered.
- Encourage State and Local agencies to include water supply in their emergency planning.

The MDEM Cyber Preparedness Unit (CPU), established under Md. Code Public Safety §14-104.1 "assists in maturing Maryland's cybersecurity posture through the development of cyber preparedness activities." The CPU assists local governments in adding a cyber annex into emergency operations plans, supports incident response planning, and provides a high-level review of cyber preparedness. The CPU is an important partner for state and local governments in preparing for cyber incidents, especially in the WWS sector.

> **RECOMMENDATION 31**: Planning for a cyber event is critical to readiness. Maryland should further leverage the CPU to help local governments plan for an incident against their WWS facilities. Encourage local governments to utilize CPU emergency response planning assistance, focusing on critical infrastructure.

2.3.3 Supply Chain and 3rd Party Risk Management

The WWS sector supply chains of physical components and digital technology are vulnerable points malicious actors can utilize to attack its systems. While manipulating the physical devices along the supply chain may be complex, it is not impossible. Additionally, devices manufactured outside of the United States could be manipulated during their manufacture and appear to be normal, functioning devices. Digital and connected devices face cyber threats similar to those in the IT network. Therefore, supply chain protection and buying devices from a reputable manufacturer are also important.

To highlight the potential risks, in October 2024, the U.S. National Cyber Director Harry Coker drew attention to the issue, noting:

> "Imagine on the supply chain side for cybersecurity. In all likelihood, we would not have the visual impact [of the Hezbollah attack] at that moment. But we should never rest easy on that. We have to take supply chain security seriously early and throughout the process."[81]

The Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) created Supply Chain Cybersecurity Principles to "characterize the foundational actions and approaches needed to deliver strong cybersecurity throughout the vast global supply chains that build energy automation and industrial control systems (ICS)." While designed for the energy sector, the WWS sector can also utilize the principles.

Additionally, it is important to note that companies publicly supporting the DOE principles produce products for use in the WWS sector. For example, Rockwell Automation is a signatory

---

[81] Jonathan Greig, "National Cyber Director Warns of Ransomware, Chinese Infrastructure Attacks and Cyber Supply Chain Concerns," The Record. Recorded Future News, October 9, 2024, https://therecord.media/national-cyber-director-coker-warns-ransomware-supply-chain-attacks-china-critical-infrastructure.

offering smart water solutions and highlighting its OT cybersecurity focus. Rockwell is just one example of several, and those seeking to digitally transform their WWS OT should consider products designed with security in mind.

> **RECOMMENDATION 32**: Encourage Maryland WWS members to become familiar with and apply the DOE Supply Chain Cybersecurity Principles. Additionally, encourage the WWS sector to seek products designed with cybersecurity in mind.

2.3.3.1 Third Party

As part of a comprehensive cybersecurity strategy, organizations must consider the third-party aspects of their operation and internal controls and develop a third-party risk management plan.

> "A third party is any external company, individual, or other entity that provides goods or services to your organization. Your business relies on these external entities, which include suppliers, vendors, contractors, service providers, and business partners, to conduct regular operations."[82]

In the WWS Sector, third parties include equipment manufacturers, hardware and software vendors, consultants, logistics services, chemical vendors, and many others. Anyone outside of the organization who provides goods or services or has access to the facility and network is a third party that must be considered when securing the operation.

The WWS facility must account for the digital aspects of their devices and equipment and how the third-party addresses cybersecurity. Additionally, the facility should have a strategy to limit third-party access on-site and ensure that a facility representative is aware of the activities conducted. While the third party may be a trusted partner, accidents can happen. A compromised device could be inadvertently introduced into the WWS facility network, such as plugging in a thumb drive. While the act was malicious, the outcome could initiate a cyber incident.

The Maryland WWS Sector should have a plan to address third-party risks, including cybersecurity risks, during contract negotiations.

> **RECOMMENDATION 33**: MDE, in partnership with DoIT and the MLCC, should ensure WWS Sector operators know the third-party risk to their facilities and networks and take proactive measures to limit the potential for the third party to be a cyber attack vector.

---

[82] Matthew Delman, "What Are Vendors & Suppliers in Third-Party Risk Management?," Prevalent, Inc, February 1, 2024, https://www.prevalent.net/blog/third-party-vendors-suppliers/.

2.4 Resource Management

2.4.1 Financial, Human, and Cyber Resources

2.4.1.1 Funding Cybersecurity Upgrades

Hiring cybersecurity staff can be expensive, and smaller localities may not have the resources to afford to hire a full-time or contract information security officer. Following the enactment of Maryland Senate Bill 754, The Local Cybersecurity Support Act of 2022, which established specific obligations for units of local governments and introduced support programs to assist them, the Department of Information Technology (DoIT), under the Director of Local Cybersecurity, established the Information Security Officer (ISO) program.

The program, now known as The Local Cyber Program, is designed to meet SB754 requirements, including compliance with the State Minimum Cybersecurity Standards. Additionally, the program seeks to improve overall cybersecurity posture and resiliency across local government units. The Director has hired subject matter experts to conduct cybersecurity assessments using the NIST CSF to identify weaknesses, provide remediation plans, and then engage with the entity to mitigate the weaknesses. The Director seeks to bring all Counties and schools into compliance and alignment with the State standards.

To address the need to provide greater assistance to the critical infrastructure sectors, the Director and his team are standing up the WWS Sector working group, as highlighted previously in this report. This group will seek ways to provide assistance and solutions to the CI sector. The director is also exploring hiring security engineers specialized in OT and ICS to directly support CI's cybersecurity programs.

> **RECOMMENDATION 34**: The State of Maryland should increase funding to the Local Cyber Program, specifically for a cybersecurity sprint targeting the WWS Sector to identify weaknesses and assist with security improvements. The funding should be robust, allowing the program to address issues within other sectors following the WWS Sector.

2.4.1.2 Economic Value of Prevention

> "Every critical infrastructure organization should double down on their commitment to resilience. CEOs, Boards, and every business leader must recognize that they own cyber risk as a business risk and a matter of good governance. They must expect disruption, continually testing the continuity of critical systems and functions to ensure they can operate through disruption and recover rapidly from an attack."
>
> -- Jen Easterly, Director, CISA

On average, preventing a cyber attack is less expensive than remediating an attack. In 2020, the Ponemon Institute found in a survey that 18 percent of the cost of cybersecurity was

prevention, and 82 percent was response and remediation.[83] Thus, an organization saved 82 percent on average through upfront cybersecurity investments. While prevention will always be a cost center, up-front investment into cybersecurity saves time and money.

As previously noted earlier in this report, education and awareness are important for executive leadership and management of a WWS sector facility or the government or company controlling the facility. A better understanding of the value of prevention and the need to invest in security can lessen the financial burden of protecting a facility.

> **RECOMMENDATION 35:** The State of Maryland, through the MDE, should conduct a comprehensive education campaign targeted at leaders within the WWS sector, emphasizing the economic value of cybersecurity prevention over remediation.

2.4.2 Cyber Resources

Federal Government agencies offer a variety of free information and services to State and Local governments and members of the WWS sector. These resources are a good starting point for those seeking additional information and assistance, especially at low to no cost.

- EPA Cybersecurity for the Water Sector - https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector
- CISA Water and Wastewater Cybersecurity - https://www.cisa.gov/water

> **RECOMMENDATION 36:** MDE, in partnership with DoIT, should ensure that Maryland WWS Sector members know the free resources available from Federal agencies, including but not limited to those above. These resources are valuable starting points and continuing into cybersecurity maturation.

Free resources and training are available through the National Rural Water Association (NRWA) for the small and very small water systems in Maryland, including free membership to the WaterISAC through a cybersecurity collaboration between the NRWA and WaterISAC. Additionally, NRWA has partnered with the SANS Institute to offer SANS Training Modules and resources. The NRWA also started a one-year Cybersecurity Circuit Rider Program Study in November 2024 focused on ways to help small systems best.[84]

> **RECOMMENDATION 37:** MDE, in partnership with DoIT, should ensure that small and very small WWS in Maryland are aware of the NRWA resources available to them. These free resources should be especially helpful to those small systems that do not have available resources.

---

[83] Deep Instinct, "The Economic Value of Prevention," accessed November 12, 2024, https://info.deepinstinct.com/value-of-prevention.
[84] National Rural Water Association, "NRWA Announces Cybersecurity Circuit Rider Program Study," October 31, 2024, https://content.nrwa.org/home/news/15705085/national-rural-water-association-nrwa-nrwa-announces-cybersecurity-circuit-rider-program-study.

2.5 Education and Awareness

2.5.1 Cyber Education and Awareness

The organization's staff requires continuous training, support, and resources to implement secure software configurations and detect malicious activity. Staff need to continuously enhance their technical competency, gain additional institutional knowledge of their systems, and ensure are provided sufficient resources by management to adequately protect their networks. --
CISA

In November 2024, CISA provided insights from a red team assessment of a U.S. CI organization and found that staff at the organization require continuous training and the necessary resources to secure their systems.[85] Additionally, CISA highlighted the need for the organization's leadership to more fully understand cyber risks and better risk-based decision-making.

As cyber-attacks increasingly target states and local governments, government officials must be aware of cybersecurity, its role in protecting operations, and the value of proactively investing in cybersecurity protections. In March 2022, the FBI noted that local U.S. government victims tended to be among smaller counties and municipalities, likely because of their limited budgets and cybersecurity resources.[86] Therefore, increasing cybersecurity education and awareness among government officials should continue to be a key goal for the State.

RECOMMENDATION 38: The State of Maryland should continue to invest in and empower the Maryland Cybersecurity Council (MCC) to fulfill its mandate of developing and promoting consistent cybersecurity strategies across all levels of government.

Education of state and local government officials about the importance of cybersecurity is imperative to ensure awareness of the need for investment in cybersecurity. In 2016, Colorado HB16-1453, Colorado Cybersecurity Initiative, established what has since become the National Cybersecurity Center (NCC).[87] The NCC is a 501(c)3 nonprofit organization "committed to advancing pragmatic, forward-thinking security policies and programs through cybersecurity leadership, collaboration, and education." One of their programs is Cybersecurity of Government Leaders, which offers no-cost virtual training for government leaders and their staff to learn the value of "cybersecurity of their state, county, or municipality."

RECOMMENDATION 39: In partnership with MDE and DoIT, host regular training for State and Local leaders through the NCC or another organization, such as CISA, to improve cybersecurity awareness among Maryland governments.

---

[85] U.S. CISA, "Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization," November 21, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-326a.

[86] U.S. FBI, "Ransomware Attacks Straining Local US Governments and Public Services," Private Industry Notification, March 30, 2022, https://www.ic3.gov/CSA/2022/220330.pdf.

[87] Millie Hamner and Kent Lambert, "Colorado Cybersecurity Initiative," Pub. L. No. HB16-1453 (2016), https://leg.colorado.gov/sites/default/files/2016a_1453_signed.pdf.

Additional training partnerships exist and should be explored. In 2023, the State of Indiana partnered with the Indiana Section of the AWWA to provide cybersecurity training for municipal staff, local government leadership, and water and wastewater utilities in Indiana. The training was free to attendees and conducted in person and online over seven sessions. The training provided basic cybersecurity knowledge, cybersecurity risk assessment, and response planning.

Maryland is part of the Chesapeake Section of the American Water Works Association (CSAWWA), including Delaware and the District of Columbia.[88] According to CSAWWA, they represent over 900 water professionals. Based on the regional composition of the CSAWWA:

> **RECOMMENDATION 40**: Partner with the Delaware and District of Columbia governments to offer water cybersecurity training through the CSAWWA. Because the AWWA and CSAWWA "speak the language of water," they can effectively communicate the need for cybersecurity in the water sector and the associated risks.

In another example, the CISA Region 3 Cybersecurity Advisors (CSAs) in Pennsylvania partnered with a Maryland-based cybersecurity firm to highlight free OT security services available through the company to Pennsylvania utilities. CISA does not endorse the specific company; however, as part of its mission, CSAs "introduce organizations to various CISA cybersecurity products and services, along with other public and private resources." Of note, Maryland also falls within CISA Region 3.[89]

> **RECOMMENDATION 41**: Following the established model in Pennsylvania, the DoIT MLCC, in partnership with MDE should consider partnering with CISA Region 3 CSAs to highlight private resources available to the Maryland WWS Sector.

Further, identifying adequate cybersecurity training for local government can be challenging, given the wide range of potential options. To help local governments readily identify and select training, the State of Texas under TX Govt Code § 2054.001 (2023), Sec. 2054.519, directed its Department of Information Resources, in consultation with their state cybersecurity council, to certify at least five cybersecurity training programs that state and local government employees could use.[90]

> **RECOMMENDATION 42**: Recommend that the Maryland DoIT certify cybersecurity training programs that local governments could select to train their staff, including those responsible for WWS facilities.

Within Maryland DoIT, under the leadership of the Director of Local Cybersecurity, the Maryland Local Cybersecurity Collaborative (MLCC) works to bring security personnel from local jurisdictions across the State to share cybersecurity information and resources. Additionally, the MLCC established a Water/Wastewater Community of Practice specifically focused on this

---

[88] "Home," CSAWWA, http://www.csawwa.org/home.html.
[89] U.S. CISA, "Region 3," https://www.cisa.gov/about/regions/region-3.
[90] State of Texas, "GOVERNMENT CODE CHAPTER 2054. INFORMATION RESOURCES," accessed November 12, 2024, https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm.

sector. These efforts are important to build a strong community within Maryland focused on securing the WWS sector.

> **RECOMMENDATION 43**: The State of Maryland should further invest resources in and promote the collaborative efforts of the Director of Local Cybersecurity and the Maryland Local Cybersecurity Collaborative (MLCC) to enhance cybersecurity awareness and capabilities within local governments. This communication pathway can serve as a vital cybersecurity accelerator within local governments.

Maryland's universities are a valuable resource for cybersecurity experts, knowledge, and training. For example, The University of Maryland Advanced Cybersecurity Experience for Students (ACES) was established "to provide students with the interdisciplinary skills needed for cybersecurity roles, combining computer science, business and public policy." Educating future cybersecurity professionals is critical to helping reduce the cybersecurity skills gap. In another example, the University of Maryland, Baltimore County School of Public Policy, has conducted research to understand and improve local government cybersecurity. Researchers created "Cybersecurity for Local Government: A Primer," which is "about cybersecurity specifically for elected officials and top managers in American local governments."

> **RECOMMENDATION 44**: The State of Maryland should actively leverage its universities' cybersecurity resources and expertise to enhance cybersecurity awareness and education across all levels of government and critical infrastructure sectors, especially the WWS sector. These centers of excellence can help secure Maryland CI.

Further, by leveraging the expertise of Maryland university experts, professional development courses for CI can be created. Partnerships with the universities can provide students with real-world experience through opportunities for class projects to help WWS Sector facilities evaluate their cybersecurity, provide technical assistance, and develop training materials.

For example, the Georgia Institute of Technology partnered with the Pacific Northwest National Laboratory to create the Institute for Cybersecurity and Resilient Infrastructure Studies (ICARIS). ICARIS aims to "deliver the technologies, test-beds, and talent necessary to secure the nation's critical infrastructure." This effort includes developing future workforce and providing advice and solutions to "communities, states, federal agencies, and businesses."

Federal grant funding to establish and fund a training program is a potential option. The University of Memphis received a $2M grant from the National Security Agency's National Centers of Academic Excellence in Cybersecurity (NCAE-C) program for a research-based Cybersecurity Education Innovation project.[91] The University formed a consortium with the University of West Florida, North Carolina A&T State University, and The Citadel to improve critical infrastructure cybersecurity focused on the southeast region and nation.

Further, following the clinic model utilized by law schools, several universities, such as UC Berkeley, MIT, Indiana University, and the University of Alabama, created cybersecurity clinics

---

[91] The University of Memphis, "Cybersecurity Education in Critical Infrastructure Protection," UNIVERSITY OF MEMPHIS RECEIVES $2M CRITICAL INFRASTRUCTURE CYBERSECURITY GRANT, August 2021, https://www.memphis.edu/cfia/projects/cecip.php.

and came together in 2021 to launch the Consortium of Cybersecurity Clinics. The Consortium shares knowledge and "lowers the barriers for other institutions to establish their own clinics."[92] Clinics provide services to organizations in their regions while providing students with real-world cybersecurity experience. According to the Consortium, clinics cost approximately $300,000 to establish and $100,000 per year after to operate. Within Maryland, the UMBC Cybersecurity Clinic, part of the UMBC Cybersecurity Institute (UCI), has become a member of The Consortium.[93]

Specifically focused on improving water system cybersecurity, the State of Indiana Office of Technology (IoT) partnered with Purdue University and Indiana University (IU) to create Cybertrack, which provides cybersecurity assessments to local governments.[94] In December 2024, IoT announced that Cybertrack would offer free cybersecurity assessments to water and wastewater treatment facilities.[95]

> **RECOMMENDATION 45**: Following the cybersecurity clinic model, the State of Maryland should partner with Maryland Universities to create a CI-focused cybersecurity training and consulting program specifically targeting OT, converged technologies, and CI, especially the WWS sector.

The University of Maryland School of Public Policy also developed the course PLCY388C Special Topics in Public Policy; Cybersecurity Policy: Practical Hacking for Policymakers.[96] This course educates undergraduate students on "key issues facing policymakers attempting to manage the problem of cybersecurity from its technical foundations to domestic and international policy considerations surrounding governance, privacy, risk management, and operational orchestration."

> **RECOMMENDATION 46**: The State of Maryland, in partnership with the University of Maryland School of Public Policy, should develop and offer a specialized executive education program based on the PLCY388C course ("Cybersecurity Policy: Practical Hacking for Policymakers"). Tailoring this program for a professional audience of state and local government leaders is important.

In addition to Maryland universities, TEDCO (Maryland Technology Development Corporation) would be another organization with which to partner for CI cybersecurity training efforts. The Cyber Maryland Program, through TEDCO, seeks to address workforce vacancies in the state and could help increase the number of those with OT cybersecurity training.[97]

---

92 The Consortium of Cybersecurity Clinics. "Consortium of Cybersecurity Clinics," n.d. https://cybersecurityclinics.org/.
93 UMBC Cybersecurity Clinic - https://cybersecurity.umbc.edu/cybersecurity-clinic/
94 Indiana Cybertrack. "Cybertrack," n.d. https://incybertrack.org/.
95 Wood, Colin. "Indiana Begins Offering Water Systems Free Cyber Assessments." *StateScoop* (blog), December 3, 2024. https://statescoop.com/indiana-begins-offering-water-systems-free-cyber-assessments/.
96 UMD School of Public Policy, "PLCY388C," accessed November 13, 2024, https://spp.umd.edu/your-education/courses/plcy388c.
97 TEDCO, "Cyber Maryland Program," https://www.tedcomd.com/resources/government-program-development-affairs-policy/cyber-maryland-program.

2.5.2 Cyber Threat Intelligence (CTI)

According to Microsoft, "threat intelligence is important because it helps organizations prioritize the strategies and tactics that will better protect them against a dynamic threat landscape."[98] Threat intelligence is available at various levels and provides key insights into cyber actors' groups, techniques, and targets. CTI also provides known indicators to help identify and guard against attempted attacks.

Threat intelligence is also available through various sources, both free and paid. Within Maryland, the Maryland Information Sharing and Analysis Center (MD-ISAC) provides CTI to Maryland-based governmental organizations or other governmental organizations that have a direct relationship with the State of Maryland. Senate Bill 754 in 2022 directed the establishment of the MD-ISAC and noted that it shall "COORDINATE INFORMATION ON CYBERSECURITY BY SERVING AS A CENTRAL LOCATION FOR INFORMATION SHARING ACROSS STATE AND LOCAL GOVERNMENT, FEDERAL GOVERNMENT PARTNERS, AND PRIVATE ENTITIES."[99]

According to the MD-ISAC website, to join the MD-ISAC organization, "the requesting agency must be a Maryland-based governmental organization or another governmental organization that has a direct relationship with the State of Maryland."[100] Private CI companies should be allowed to join to strengthen cybersecurity within Maryland.

> **RECOMMENDATION 47**: DoIT and the MD-ISAC should allow all Maryland CI companies to join to strengthen further cybersecurity and information sharing within all portions of each sector.

Another option is the Multi-State Information Sharing and Analysis Center (MS-ISAC), which offers free CTI and services to U.S. State, Local, Tribal, and Territorial (SLTT) government organizations and additional fee-based services.[101] Additionally, the federal government issues cyber alerts through CISA and several other agencies, as well as partnerships with other countries, such as the UK.

Specifically, for the WWS sector, the WaterISAC "is the only all-threats security information source for the water and wastewater sector." While the WaterISAC is a non-profit organization, one potential barrier for systems to join is the annual dues.[102] The dues are based on the size of the system but create the need for those responsible for the WWS system budget to provide funding for the system to join.

---

[98] Microsoft Security, "What Is Cyber Threat Intelligence?," What is cyber threat intelligence?, https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-threat-intelligence.
[99] https://mgaleg.maryland.gov/2022RS/bills/sb/sb0754E.pdf
[100] Maryland DoIT, "MD-ISAC," n.d., https://doit.maryland.gov/cybersecurity/Pages/default.aspx.
[101] Center for Internet Security, "Multi-State Information Sharing and Analysis Center," https://www.cisecurity.org/ms-isac/.
[102] WaterISAC, "Become a WaterISAC Member," https://www.waterisac.org/membership.

RECOMMENDATION 48: MDE and DoIT should encourage municipalities to leverage the Maryland State and Local Cybersecurity Grant Program (SLCGP) in 2025 to apply for funding and consider using part of those funds to join the WaterISAC.

While CTI from internal and external sources is a critical part of the organization's cybersecurity, it is also imperative that the organization can understand the information and know how to utilize the information it receives. Developing a library of CTI without being able to implement and action the information does not increase organizational security.

RECOMMENDATION 49: As part of state outreach and education efforts conducted by the MLCC, provide organizations assistance in understanding CTI and how they can operationalize the information. The MLCC is a strong group that can help achieve this goal.

To further help organizations understand the tactics, techniques, and procedures used by adversaries that are often detailed in CTI, the MITRE ATT&CK® Matrix for ICS provides a "knowledge base of adversarial techniques based on real-world observations."[103] This Matrix can help organizations defend against cyber attacks by reviewing known methodologies attackers use.

2.5.3 Cyber Portal

Residents and businesses operating within Maryland should have a central cybersecurity portal to find information and resources within the State. While websites exist and provide cyber information, combining this information in a comprehensive website would enable faster discovery of information and resources. Under the Office of Security Management (OSM) within the DoIT, a cybersecurity website exists and would be a strong starting point to update with additional information. This website should also become the central point of information within the State.

RECOMMENDATION 50: The Maryland DoIT Office of Security Management (OSM), headed by the State Chief Information Security Officer (CISO), should develop and maintain a comprehensive cybersecurity information and resource portal for Maryland residents and businesses. An easy-to-identify website, such as **cyber.maryland.gov**, would also be a helpful URL.

Given the interconnectedness of the National Capitol Region and water systems, which share a water supply, collaboration and coordination between the State and Local governments of the region will help strengthen security.

RECOMMENDATION 51: The State of Maryland should lead a regional partnership among states and the District of Columbia in the National Capital Region to leverage resources and share best practices to strengthen the cybersecurity of the WWS sectors in the area.

---

[103] The MITRE Corporation, "Matrix - ICS | MITRE ATT&CK®," https://attack.mitre.org/matrices/ics/.

APPENDIX A: Consolidated Recommendations List

RECOMMENDATION 1: Officially designate the MDE as the lead agency for coordinating security efforts within the Maryland WWS sector. Additionally, MDE should coordinate with other State agencies regarding cybersecurity policies and efforts targeting the WWS sector.

RECOMMENDATION 2: The State of Maryland should affirm support for the MDE plan to include the cybersecurity awareness component for all new and renewing operator and superintendent certifications.

RECOMMENDATION 3: Amend Code of Maryland Regulations (COMAR) Quality of Drinking Water in Maryland, 26.26.04.01, to include a comprehensive section regarding cybersecurity standards for water and wastewater treatment facilities.[104]

RECOMMENDATION 4: Supplement the Modernize Maryland Act of 2022 with a new Act to address cybersecurity vulnerabilities in the greater Maryland WWS sector. Modeling after the Minnesota EO, require PWSs in the state that use OT to conduct an annual cybersecurity assessment and certify compliance with the MDE.

RECOMMENDATION 5: The State of Maryland should formally express its support for developing and implementing a robust national cybersecurity policy covering the entirety of the WWS sector. The plan should be tailored to the specific needs of the WWS sector, and support should highlight the benefits of a national strategy to reduce cyber risk instead of requiring states to work independently.

RECOMMENDATION 6: Recommend that the AI Subcabinet, in coordination with Maryland DoIT and the MCC Critical Infrastructure Subcommittee, examine AI's impact on Maryland CI, including the WWS sector. Recommend providing guidance for the sector to utilize AI and defend against AI-enabled threats.

RECOMMENDATION 7: Amend Code of Md. Regs. Quality of Drinking Water in Maryland. 26, § 26.04.01.19, Reporting Requirements, to include a requirement that a supplier of water report cyber incidents within 24 hours.

RECOMMENDATION 8: Recommend WWS sector facilities create and maintain a robust cyber incident reporting program and include the program in annual security training.

RECOMMENDATION 9: Allocate funding, or seek grants, to enable the Maryland Department of Emergency Management (MDEM) to create a cyber-focused CERC plan for Maryland, especially the WWS sector. Alternatively, consider leveraging the California plan.

RECOMMENDATION 10: Include cybersecurity attack information on the MDEM "Know the Threats" website and consider the MD Ready as an alerting system if required.

---

[104] Chapter 01 Quality of Drinking Water in Maryland
https://mde.maryland.gov/programs/regulations/water/Documents/26.04.01.01%2C%20.01-1%2C%20.20%2C%20and%20.37.pdf

RECOMMENDATION 11: MDE should encourage/require each WWS sector facility, or managing government or office, to appoint a primary point of contact for cybersecurity.

RECOMMENDATION 12: The State of Maryland should amend its Public Information Act (PIA) § 4-338 to explicitly exempt sensitive security and infrastructure information voluntarily provided to state agencies. Recommend expanded wording which notes, "a custodian shall deny inspection of the part of a public record that contains information about the security of an information system or critical infrastructure system."

RECOMMENDATION 13: Maryland should consider enacting a privacy act focusing on smart meters and utilities and informing residents about their options to protect their privacy.

RECOMMENDATION 14: MDE should implement measures to protect the "List of Active Certified Operators" maintained on its website while ensuring legitimate access for necessary purposes.

RECOMMENDATION 15: MDE, in partnership with DoIT, should recommend that the WWS sector adopt basic cyber hygiene practices, such as those outlined in CIS Critical Security Controls, to help address security gaps and strengthen the sector.

RECOMMENDATION 16: MDE, in partnership with DoIT, should encourage the WWS sector to adopt best practices, including password and identity management, and network segmentation. WWS systems should also ensure that they reduce cyber vulnerabilities.

RECOMMENDATION 17: Ensure WWS sector facilities are aware of the "Top Cyber Actions for Securing Water Systems" fact sheet and help direct them to additional resources as needed.

RECOMMENDATION 18: MDE, in collaboration with the Maryland Cybersecurity Coordinating Council (MCCC), should actively promote and support the implementation of CISA's "Top Cyber Actions for Securing Water Systems" fact sheet by all Water and Wastewater Systems (WWS) in Maryland.

RECOMMENDATION 19: Recommend WWS entities and those responsible for their IT and OT adopt a ZT security model and leverage the ZT materials provided by the U.S. government as free resources.

RECOMMENDATION 20: Through DoIT's cybersecurity portal, improve awareness of Secure by Design features among Maryland State and Local Government officials and private water companies. MDE should encourage WWS sector facilities to select upgraded equipment that meets Secure by Design principles when available.

RECOMMENDATION 21: MDE should recommend WWS organizations in Maryland implement NIST CSF 2.0 to improve cybersecurity. Adoption of a framework can help an organization reduce its cyber risk.

RECOMMENDATION 22: MDE should encourage the WWS sector in Maryland to follow NIST SP 800-82r3 and implement NIST's security recommendations.

RECOMMENDATION 23:MDE should recommend that WWS organizations in Maryland adopt a reference model appropriate for their OT network to guide security improvements.

RECOMMENDATION 24: MDE, in collaboration with the Maryland Cybersecurity Council (MCC) and DoIT, should develop and promote a guidance document that outlines recommended cybersecurity frameworks and standards for WWS in Maryland.

RECOMMENDATION 25: Encourage the WWS sector members to become familiar with the six principles to ensure proper cybersecurity controls are in place. MDE and DoIT should partner to offer education and training regarding methods to implement these principles.

RECOMMENDATION 26: MDE should recommend that all Maryland WWS Sector facilities follow physical security best practices throughout their facility and remote locations. Additionally, systems should regularly review their physical security posture and make changes and improvements as necessary.

RECOMMENDATION 27: MDE should expand the Emergency Response Plans (ERPs) requirement to include cybersecurity provisions for all community water systems (CWS).

RECOMMENDATION 28: The MDE should actively promote adopting and utilizing the EPA's Incident Action Checklist – Cybersecurity by all WWS in Maryland.

RECOMMENDATION 29: MDE, in partnership with MDEM and DoIT, should regularly host tabletop exercises tailored to the Maryland WWS sector to continue refining state and local government responses to cyber incidents.

RECOMMENDATION 30: As part of MDEM's planning, ensure that:

- Planning occurs specifically for cyber incidents impacting the WWS sector, especially those that may disrupt water service to Maryland residents and businesses.
- Plans for alternative water supplies and mutual aid agreements should water services be unavailable, and the community require water needs to be delivered.
- Encourage State and Local agencies to include water supply in their emergency planning.

RECOMMENDATION 31: Planning for a cyber event is critical to readiness. Maryland should further leverage the CPU to help local governments plan for an incident against their WWS facilities. Encourage local governments to utilize CPU emergency response planning assistance, focusing on critical infrastructure.

RECOMMENDATION 32: Encourage Maryland WWS members to become familiar with and apply the DOE Supply Chain Cybersecurity Principles. Additionally, encourage the WWS sector to seek products designed with cybersecurity in mind.

RECOMMENDATION 33: MDE, in partnership with DoIT and the MLCC, should ensure WWS Sector operators know the third-party risk to their facilities and networks and take proactive measures to limit the potential for the third party to be a cyber attack vector.

RECOMMENDATION 34: The State of Maryland should increase funding to the Local Cyber Program, specifically for a cybersecurity sprint targeting the WWS Sector to identify weaknesses and assist with security improvements. The funding should be robust, allowing the program to address issues within other sectors following the WWS Sector.

RECOMMENDATION 35: The State of Maryland, through the MDE, should conduct a comprehensive education campaign targeted at leaders within the WWS sector, emphasizing the economic value of cybersecurity prevention over remediation.

RECOMMENDATION 36: MDE, in partnership with DoIT, should ensure that Maryland WWS Sector members know the free resources available from Federal agencies, including but not limited to those above. These resources are valuable starting points and continuing into cybersecurity maturation.

RECOMMENDATION 37: MDE, in partnership with DoIT, should ensure that small and very small WWS in Maryland are aware of the NRWA resources available to them. These free resources should be especially helpful to those small systems that do not have available resources.

RECOMMENDATION 38: The State of Maryland should continue to invest in and empower the Maryland Cybersecurity Council (MCC) to fulfill its mandate of developing and promoting consistent cybersecurity strategies across all levels of government.

RECOMMENDATION 39: In partnership with MDE and DoIT, host regular training for State and Local leaders through the NCC or another organization, such as CISA, to improve cybersecurity awareness among Maryland governments.

RECOMMENDATION 40: Partner with the Delaware and District of Columbia governments to offer water cybersecurity training through the CSAWWA. Because the AWWA and CSAWWA "speak the language of water," they can effectively communicate the need for cybersecurity in the water sector and the associated risks.

RECOMMENDATION 41: Following the established model in Pennsylvania, the DoIT MLCC, in partnership with MDEM, should consider partnering with CISA Region 3 CSAs to highlight private resources available to the Maryland WWS Sector.

RECOMMENDATION 42: Recommend that the Maryland DoIT certify cybersecurity training programs that local governments could select to train their staff, including those responsible for WWS facilities.

RECOMMENDATION 43: The State of Maryland should further invest resources in and promote the collaborative efforts of the Director of Local Cybersecurity and the Maryland Local Cybersecurity Collaborative (MLCC) to enhance cybersecurity awareness and capabilities within local governments. This communication pathway can serve as a vital cybersecurity accelerator within local governments.

RECOMMENDATION 44: The State of Maryland should actively leverage its universities' cybersecurity resources and expertise to enhance cybersecurity awareness and education across all levels of government and critical infrastructure sectors, especially the WWS sector. These centers of excellence can help secure Maryland CI.

RECOMMENDATION 45: Following the cybersecurity clinic model, the State of Maryland should partner with Maryland Universities to create a CI-focused cybersecurity training and consulting program specifically targeting OT, converged technologies, and CI, especially the WWS sector.

RECOMMENDATION 46: The State of Maryland, in partnership with the University of Maryland School of Public Policy, should develop and offer a specialized executive education program based on the PLCY388C course ("Cybersecurity Policy: Practical Hacking for Policymakers"). Tailoring this program for a professional audience of state and local government leaders is important.

RECOMMENDATION 47: DoIT and the MD-ISAC should allow all Maryland CI companies to join to strengthen further cybersecurity and information sharing within all portions of each sector.

RECOMMENDATION 48: MDE and DoIT should encourage municipalities to leverage the Maryland State and Local Cybersecurity Grant Program (SLCGP) in 2025 to apply for funding and consider using part of those funds to join the WaterISAC.

RECOMMENDATION 49: As part of state outreach and education efforts conducted by the MLCC, provide organizations assistance in understanding CTI and how they can operationalize the information. The MLCC is a strong group that can help achieve this goal.

RECOMMENDATION 50: The Maryland DoIT Office of Security Management (OSM), headed by the State Chief Information Security Officer (CISO), should develop and maintain a comprehensive cybersecurity information and resource portal for Maryland residents and businesses. An easy-to-identify website, such as **cyber.maryland.gov**, would also be a helpful URL.

RECOMMENDATION 51: The State of Maryland should lead a regional partnership among states and the District of Columbia in the National Capital Region to leverage resources and share best practices to strengthen the cybersecurity of the WWS sectors in the area.

APPENDIX B: Cybersecurity Resources

CISA Water and Wastewater Cybersecurity https://www.cisa.gov/water

EPA Cybersecurity for the Water Sector https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector

American Water Works Association, "Cybersecurity & Guidance," https://www.awwa.org/resource/cybersecurity-guidance/

National Rural Water Association (NRWA) Cybersecurity https://nrwa.org/issues/cybersecurity/

NIST Cybersecurity Framework 2.0 https://www.nist.gov/cyberframework

CISA Cybersecurity Performance Goals (CPGs) https://www.cisa.gov/cybersecurity-performance-goals-cpgs

Strategies to Mitigate Cyber Security Incidents https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents

Essential Eight https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

Essential Eight Maturity Model https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

Industrial Control Systems Remote Access Protocol - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/industrial-control-systems-remote-access-protocol

Principles of operational technology cyber security - https://media.defense.gov/2024/Oct/01/2003556960/-1/-1/0/PRINCIPLES_OF_OPERATIONAL_TECHNOLOGY_CYBER_SECURITY.PDF

CISA Cyber Security Evaluation Tool (CSET) https://www.cisa.gov/downloading-and-installing-cset

CISA "Protect the Physical Security of Your Digital Devices https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices

CISA Cybersecurity Best Practices for Industrial Control Systems https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-industrial-control-systems

CISA Cyber Essentials https://www.cisa.gov/resources-tools/resources/cyber-essentials

CISA Configuring and Managing Remote Access for Industrial Control Systems https://www.cisa.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf

NIST SP 800-82r3 Guide to Operational Technology (OT) Security https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

CISA Mobile Communications Best Practice Guidance

https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance

References

118th Congress. (2024, April 10). *H.R.7922 - To establish a Water Risk and Resilience Organization to develop risk and resilience requirements for the water sector*. https://www.congress.gov/bill/118th-congress/house-bill/7922

American Water Works Association. (n.d.). *Cybersecurity & Guidance*. https://www.awwa.org/resource/cybersecurity-guidance/

Australian Signals Directorate. (2024). *2023–2024 Cyber threat trends For critical infrastructure*. https://www.cyber.gov.au/sites/default/files/2024-11/2023-24-cyber-threat-trends-for-critical-infrastructure.pdf

Bartock, Michael, Jeffrey Cichonski, Murugiah Souppaya, Matthew Smith, Greg Witte, and Karen Scarfone. "Guide for Cybersecurity Event Recovery." Gaithersburg, MD: National Institute of Standards and Technology, 2016. https://doi.org/10.6028/NIST.SP.800-184.

Belal, S. M. (n.d.). *The Top 7 Operational Technology Patch Management Best Practices* [Blog]. ISA Global Cybersecurity Alliance. https://gca.isa.org/blog/the-top-7-operational-technology-patch-management-best-practices

Bigelow, S. J. (n.d.). *What is IT/OT convergence? Everything you need to know*. Search IT Operations. Retrieved November 14, 2024, from https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence

California State Water Resources Control Board. (n.d.-a). *Water Resiliency - Crisis and Emergency Risk Communication (CERC)*. https://www.waterboards.ca.gov/drinking_water/certlic/drinkingwater/water_resiliency/prepare.html#cerc

California State Water Resources Control Board. (n.d.-b). *Water Resiliency - Crisis and Emergency Risk Communication (CERC)*. https://www.waterboards.ca.gov/drinking_water/certlic/drinkingwater/water_resiliency/prepare.html#cerc

Colorado Attorney General. (n.d.). *Colorado Privacy Act (CPA)*. Retrieved November 13, 2024, from https://coag.gov/resources/colorado-privacy-act/

Colorado Cybersecurity Initiative, Nos. HB16-1453 (2016). https://leg.colorado.gov/sites/default/files/2016a_1453_signed.pdf

Deep Instinct. (n.d.). *The Economic Value of Prevention*. Retrieved November 12, 2024, from https://info.deepinstinct.com/value-of-prevention

Delman, M. (2024, February 1). *What Are Vendors & Suppliers in Third-Party Risk Management?* Prevalent, Inc. https://www.prevalent.net/blog/third-party-vendors-suppliers/

Easterly, J. (2025, January 15). *Strengthening America's Resilience Against the PRC Cyber Threats*. https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

Edge Editors. (2024, September 25). *NIST Drops Password Complexity, Mandatory Reset Rules*. Dark Reading. https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules

Fortinet Training Institute. (2024). *2024 Cybersecurity Skills Gap* (p. 30). https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

Fox-Sowell, Sophia. (2024, February 1). Where's the federal legislation for state water utility cybersecurity? *StateScoop*. https://statescoop.com/state-water-utility-cybersecurity-federal-legislation/

Governor Wes Moore. (2024). *EXECUTIVE ORDER 01.01.2024.02 Catalyzing the Responsible and Productive Use of Artificial Intelligence in Maryland State Government*. https://governor.maryland.gov/Lists/ExecutiveOrders/Attachments/31/EO%2001.01.2024.02%20Catalyzing%20the%20Responsible%20and%20Productive%20Use%20of%20Artificial%20Intelligence%20in%20Maryland%20State%20Government_Accessible.pdf

Greig, J. (2024, October 9). *National cyber director warns of ransomware, Chinese infrastructure attacks and cyber supply chain concerns*. The Record. Recorded Future News. https://therecord.media/national-cyber-director-coker-warns-ransomware-supply-chain-attacks-china-critical-infrastructure

Guri, M. (2024). *Mind The Gap: Can Air-Gaps Keep Your Private Data Secure?* arXiv. https://doi.org/10.48550/ARXIV.2409.04190

Hanssen, G. K., Thieme, C. A., Bjarkø, A. V., Lundteigen, M. A., Bernsmed, K. E., & Jaatun, M. G. (2023). *A continuous OT cybersecurity risk analysis and Mitigation process*. Research Publishing Services. https://doi.org/10.3850/978-981-18-8071-1_P413-cd

Harrell, B., & Le, J. (2025, January 17). Restoring U.S. cyber resilience: A blueprint for the new administration. *CyberScoop*. https://cyberscoop.com/restoring-u-s-cyber-resilience-trump-administration-brian-harrell-jeff-le-op-ed/

Home. (n.d.). CSAWWA. Retrieved November 19, 2024, from http://www.csawwa.org/home.html

Horne, Dr. R. (2024, December 3). *NCSC CEO's speech to mark the launch of the NCSC Annual Review 2024* [Speech]. https://www.ncsc.gov.uk/speech/ncsc-annual-review-launch-2024-ceo-dr-richard-horne

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*, *14*(13), 5501. https://doi.org/10.3390/app14135501

Jacobs, J., & Haney, J. (2024). Learning, Sharing, and Exploring with NIST's New Human-Centered Cybersecurity Community of Interest. *NIST*. https://www.nist.gov/blogs/cybersecurity-insights/learning-sharing-and-exploring-nists-new-human-centered-cybersecurity

Jockims, T. L. (2024, June 26). *America's drinking water is facing attack, with links back to China, Russia and Iran*. CNBC. https://www.cnbc.com/2024/06/26/americas-drinking-water-under-attack-china-russia-and-iran.html

Lopez, C. T. (2024, May 2). *Good Cyber Hygiene Can Impede Adversary Meddling in U.S. Infrastructure*. DOD News. https://www.defense.gov/News/News-Stories/Article/Article/3763862/good-cyber-hygiene-can-impede-adversary-meddling-in-us-infrastructure/

Lyons, Jessica. "EPA Rescinds US Water Cybersecurity Rule after Legal Battle." The Register, October 13, 2023. https://www.theregister.com/2023/10/13/epa_rescinds_water_cybersecurity_rule/.

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. *IEEE Access*, *9*, 165295–165325. https://doi.org/10.1109/ACCESS.2021.3133348

Maryland Department of the Environment. (n.d.). *Emergency Response Home*. Department of the Environment. https://mde.maryland.gov/programs/crossmedia/EmergencyResponse/Pages/default.aspx

Maryland DoIT. (n.d.). *MD-ISAC*. https://doit.maryland.gov/cybersecurity/Pages/default.aspx

Maryland General Assembly. (2022, May 11). *State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022)*. https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/Hb1205/?ys=2022rs

Maryland MDE. (n.d.). *Laws and Regulations Governing the MDE Water Supply Program*. Retrieved November 12, 2024, from https://mde.maryland.gov/programs/water/water_supply/Pages/default.aspx

Maryland Office of People's Counsel. (n.d.). *Smart Meters*. https://opc.maryland.gov/Consumer-Learning/Electricity/Smart-Meters

Microsoft Security. (n.d.). *What Is Cyber Threat Intelligence?* What Is Cyber Threat Intelligence? Retrieved November 19, 2024, from https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-threat-intelligence

Miller, K. (2024, April 19). *Rural Texas towns report cyberattacks that caused one water system to overflow*. The Texas Tribune. https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/

Minnesota IT Services. (n.d.). *Executive Order 22-20 Summary*. https://mn.gov/mnit/government/policies/security/eo22-20.jsp#:~:text=Executive%20Order%2022-20%20requires,across%20the%20State%20of%20Minnesota

National Rural Water Association. (2024, October 31). *NRWA Announces Cybersecurity Circuit Rider Program Study*. https://content.nrwa.org/home/news/15705085/national-rural-water-association-nrwa-nrwa-announces-cybersecurity-circuit-rider-program-study

Office of the Director of National Intelligence. (2024). *Annual Threat Assessment of the U.S. Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

OpenAI. (2024). *Influence and cyber operations: an update*. https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf

Otto, G. (2024, December 27). *White House: Salt Typhoon hacks possible because telecoms lacked basic security measures*. CyberScoop. https://cyberscoop.com/salt-typhoon-telecom-cybersecurity-gaps-white-house-response/

Rashotte, R. (2024, October 30). *3 key factors to make your cybersecurity training a success*. https://www.weforum.org/stories/2024/10/3-key-factors-to-make-your-cybersecurity-training-a-success/

Reagan, M. S., & Sullivan, J. (2024). *Letter to Governors*. The White House. https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf

Robins-Early, N. (2024, July 24). CrowdStrike global outage to cost US Fortune 500 companies $5.4bn. *The Guardian*. https://www.theguardian.com/technology/article/2024/jul/24/crowdstrike-outage-companies-cost

Rodriguez, R. (2024, October 15). *American Water Reactivating Systems After Cyber Event*. AP News. https://apnews.com/press-release/ein-presswire-newsmatics/camden-d80e4d4bb41e95a0c64847593b34ac20

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Smith, C. (2024, November 21). Millions of people replaced passwords with passkeys, so why haven't you? *BGR*. https://bgr.com/tech/millions-of-people-replaced-passwords-with-passkeys-so-why-havent-you/

State of Texas. (n.d.). *GOVERNMENT CODE CHAPTER 2054. INFORMATION RESOURCES*. Retrieved November 12, 2024, from https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to Operational Technology (OT) security* (No. NIST SP 800-82r3; p. NIST SP 800-82r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-82r3

TEDCO. (n.d.). *Cyber Maryland Program*. https://www.tedcomd.com/resources/government-program-development-affairs-policy/cyber-maryland-program

Temoshok, D., Fenton, J., Choong, Y.-Y., Lefkovitz, N., Regenscheid, A., & Richer, J. (2024). *Digital Identity Guidelines: Authentication and Authenticator Management* (No. NIST SP 800-63B-4 2pd; p. NIST SP 800-63B-4 2pd). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B-4.2pd

The Center for Internet Security. (n.d.). *Multi-State Information Sharing and Analysis Center*. https://www.cisecurity.org/ms-isac/

The Center for Internet Security, Inc., & Multi-State Information Sharing and Analysis Center. (2024). *Nationwide Cybersecurity Review* (p. 78). https://www.cisecurity.org/insights/white-papers/nationwide-cybersecurity-review-2023-summary-report

The MITRE Corporation. (n.d.). *Matrix - ICS | MITRE ATT&CK®*. Retrieved November 14, 2024, from https://attack.mitre.org/matrices/ics/

The University of Memphis. (2021, August). *Cybersecurity Education in Critical Infrastructure Protection*. UNIVERSITY OF MEMPHIS RECEIVES $2M CRITICAL INFRASTRUCTURE CYBERSECURITY GRANT. https://www.memphis.edu/cfia/projects/cecip.php

UK National Cyber Security Centre. (2024, September 26). *Why MFA matters*. https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/why-mfa-matters

UMD School of Public Policy. (n.d.). *PLCY388C*. Retrieved November 13, 2024, from https://spp.umd.edu/your-education/courses/plcy388c

U.S. CISA. (n.d.-a). *CISA Tabletop Exercise Packages*. CISA Tabletop Exercise Packages. Retrieved November 19, 2024, from https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

U.S. CISA. (n.d.). *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*. Retrieved November 12, 2024, from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

U.S. CISA. (n.d.-b). *Multifactor Authentication*. https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication

U.S. CISA. (n.d.-c). *Protect the Physical Security of Your Digital Devices*. https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices

U.S. CISA. (n.d.-d). *Region 3*. https://www.cisa.gov/about/regions/region-3

U.S. CISA. (2020, December 17). *Cybersecurity Best Practices for Industrial Control Systems*. https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-industrial-control-systems

U.S CISA. (2022). *Implementing Phishing-Resistant MFA*. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

U.S. CISA. (2024, February 7). *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* [Cybersecurity Advisory]. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

U.S. CISA. (2024a, February 23). *Top Cyber Actions for Securing Water Systems*. https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems

U.S. CISA. (2024b, October 1). *Principles of Operational Technology Cyber Security*. https://www.cisa.gov/resources-tools/resources/principles-operational-technology-cyber-security

U.S. CISA. (2024c, November 21). *Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-326a

U.S. CISA. (2025). *Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products*. U.S. National Security Agency. https://media.defense.gov/2025/Jan/13/2003626906/-1/-1/0/JOINT-GUIDE-SECURE-BY-DEMAND-PRIORITY-CONSIDERATIONS-OT-OWNERS-OPERATORS.PDF

U.S. EPA. (2015a, September 21). *Drinking Water Regulations*. https://www.epa.gov/dwreginfo/drinking-water-regulations

U.S. EPA. (2015b, September 21). *Information about Public Water Systems*. https://www.epa.gov/dwreginfo/information-about-public-water-systems

U.S. EPA. (2023a, March 3). *EPA Takes Action to Improve Cybersecurity Resilience for Public Water Systems* [News Release]. https://www.epa.gov/newsreleases/epa-takes-action-improve-cybersecurity-resilience-public-water-systems

U.S. EPA. (2023b, July 10). *Cybersecurity Planning*. https://www.epa.gov/waterresilience/cybersecurity-planning

U.S. EPA. (2024a, March 19). *Biden-Harris Administration engages states on safeguarding water sector infrastructure against cyber threats* [News Release]. https://www.epa.gov/newsreleases/biden-harris-administration-engages-states-safeguarding-water-sector-infrastructure

U.S. EPA. (2024b, May 20). *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*. https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities

U.S. EPA. (2024c, May 20). *EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water* [News Release]. https://www.epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect

U.S. EPA Office of Inspector General. (2024, November 13). *Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems*. https://www.epaoig.gov/reports/other/management-implication-report-cybersecurity-concerns-related-drinking-water-systems

U.S. FBI. (2022). *Ransomware Attacks Straining Local US Governments and Public Services* (Private Industry Notification Nos. 20220330–001; p. 7). https://www.ic3.gov/CSA/2022/220330.pdf

U.S. GAO. (2024, August 1). *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems*. https://www.gao.gov/products/gao-24-106744

Value of Water Campaign. (2017). *The Economic Benefits of Investing in Water Infrastructure*. https://uswateralliance.org/wp-content/uploads/2023/09/Economic-Impact-of-Investing-in-Water-Infrastructure_VOW_FINAL_pages_0.pdf

Vasquez, C. (2024, March 6). *Dragos CEO: Digitization in critical infrastructure will spur attacks*. CyberScoop. https://cyberscoop.com/water-digitization-critical-infrastructure-attacks/

Vasquez, C., & Vincens, A. (2023, November 29). *Pennsylvania water facility hit by Iran-linked hackers*. CyberScoop. https://cyberscoop.com/pennsylvania-water-facility-hack-iran/

Verizon Business. (2024). *2024 Data Breach Investigations Report*. http://verizon.com/dbir

WaterISAC. (2018, March 26). *Become a WaterISAC Member*. WaterISAC. https://www.waterisac.org/membership

Wood, C. (2024, December 3). Indiana begins offering water systems free cyber assessments. *StateScoop*. https://statescoop.com/indiana-begins-offering-water-systems-free-cyber-assessments/

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025* (p. 49) [Insight Report]. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Xylem. (n.d.). *Smart Water*. Retrieved November 13, 2024, from https://www.xylem.com/en-us/solutions/smart-utility-networks/smart-water/

Public Safety (2022). https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gps&section=14-104.1&enactments=false