Sarah Walker

Cybersecurity on Water Infrastructure in the United States

I: Introduction

According to the Director of National Intelligence, the Federal Bureau of Investigation, and the Department of Homeland Security, cyber-related risks serve as the primary threat facing our country's critical infrastructure systems. As we progress further and further into the fourth industrial revolution, the number of cyber assets in modern critical infrastructure is rapidly increasing, and the probability of foreign attack on these systems is rising as well. Critical infrastructure systems serve as the foundation of a functioning economy and society. Whether it is transport, energy, oil and gas, or water, humans rely on these systems not only to perform everyday tasks, but to live and breathe. As a result of the "ongoing digital transformation of the critical infrastructures' operators,[i]" it has become more important than ever to implement strong cybersecurity practices within these systems.

Already, our country has borne witness to the devastating impact of cyberattacks targeting critical infrastructure. On April 29, 2021, hackers gained access to the network of the largest fuel pipeline in the United States, Colonial Pipeline, through a ransomware attack, threatening oil supply in 17 different states and multiple airline companies. Not only did the attack hurt the U.S. economy through its impact on gas prices, but it endangered American citizens' safety, impacting individuals from Houston to the New York Harbor. Just weeks after the declaration of the attack on Colonial Pipeline, another critical industry endured a cyberattack; JBS foods, the world's largest meat producer, faced a ransomware attack, forcing the company to temporarily shut down its operations and ultimately pay eleven million dollars in ransom to hackers.[ii] These incidents, along with several others, serve as strong indications that critical infrastructure systems within the United States are vulnerable to attack, and the repercussions of such events can be extensive and extremely detrimental.

According to the US Department of Homeland Security (DHS), the water and wastewater sector (WWS) is considered to be "one of the main targets for cyberattacks among the 16 lifeline infrastructure sectors," and "safeguarding it against cybersecurity threats is considered a matter of national priority.[iii]" Safe drinking water is critical to a functioning society, economy, and environment. The impact of a cyberattack on water infrastructure systems can not only be devastating to the country's economy, but disastrous to public health. Through an analysis on current cybersecurity within the U.S. water sector, an investigation on recent cyberattacks on water systems, and an exploration of the primary challenges facing water infrastructure, it has become evident that a variety of changes should be implemented within the industry to protect the American economy and the American people, including the assembly of a national research and development center to strengthen professional knowledge, the establishment of round tables and seminars to promote effective information sharing, the creation of public-private partnerships to ease financial barriers, the institution of federally-mandated standards for water utilities companies, and the facilitation of teamwork between regulatory agencies and the water sector.

II: Overview of Water and Wastewater Infrastructure Sector in the United States

A: Water Infrastructure in the United States

The United States is comprised of 153,000 public drinking water systems and over 16,000 public wastewater treatment systems. The vast majority of the American population relies on these public systems for drinking water supply and three quarters of the population "has its sanitary sewage treated by these wastewater systems.[iv]" These systems are vital for municipal, agricultural, industrial, and household functioning. The water and wastewater sector also includes over 77,000 dams and reservoirs spanning across the U.S.. Each system within the water and wastewater sector "must be operable 24 hours a day, seven days a week.[v]" Ownership and operations of public drinking water and wastewater are both public and private; while dams and diversions structures are largely operated under the federal government, "the vast majority of the nation's water infrastructure is either privately owned or owned by non-federal units of government.[vi]" U.S. water systems range significantly in size, from supplying resources to the "nation's largest cities to small systems with just 15 connections.[vii]"

B: Cyber-based Elements of Water Infrastructure in the United States

While drinking water systems include physical components like water sources, conveyance systems, raw water storage, treatment centers, distribution systems, and monitoring operators, there are a variety of cyber elements within drinking water infrastructure as well. In order to monitor water quality, pressure, level and flow rate, water and wastewater management companies employ SCADA (supervisory control and data acquisition) systems to control and gain data on their operations. These systems are composed of a "master control unit" and "remote terminal units, located at pump stations and water tanks.[viii]" Using this data, operators are able to identify issues like overflows, leaks, or chemical imbalances, and address these issues efficiently.[ix] In addition to SCADA systems, process systems and operational controls, or "any electronic control systems related to the operations of the utility and treatment processes that are not controlled by the utility's SCADA system," and enterprise systems, "non-operational control systems such as customer billing, email, and other personnel-related applications and tools," are also included in water infrastructure's cyber assets.[x] As water optimization becomes more of a priority to American government personnel as a result of its environmental impact, these cyber assets are becoming a more critical and prominent element of U.S. water infrastructure systems.

III: Cybersecurity on Water and Wastewater Infrastructure in the United States

A: Frameworks, Guidelines, and Tools

While water infrastructure system designers and operators have historically directed their concerns on natural events like storms, blizzards and earthquakes, the tragedy of September 11, 2001 and the increasing probability of cyberattacks on water systems shifted this focus. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the

Environmental Protection Agency (EPA), and the National Security Agency (NSA) all contribute to supervision over information technology and operational technology networks, systems, and devices of U.S. Water and Wastewater Systems facilities.[xi]

Formulated in 2014, the NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity provides some protocol for operators of critical infrastructure companies aiming to strengthen their cyber assets. The framework includes categories to help critical infrastructure companies identify asset vulnerabilities and communication flow as well as "protect physical systems, manage remote access, and protect data.[xii]" It "can allow operators to prioritize replacement of systems, or develop more rigorous risk management practices.[xiii]" Additionally, after publishing an updated version of their framework in 2018, NIST now provides special publications and webinars on computer security, cybersecurity practice guides, and computer systems technology.[xiv]

The AWWA (American Water Works Association) also developed a framework to increase security in water-based industrial control systems in order "to inform utilities about ways to strengthen resilience" against cyberattacks;[xv] The guidelines plan "to have Industrial Control Systems (ICS) for critical applications designed, installed and maintained to protect water systems against attack and ensure no loss of operation.[xvi]" The framework establishes a ten year plan with a variety of goals including: "development and deployment of ICS security programs, development of risk assessment tools and methodologies towards determining threat and consequence analysis, and developing and implementing risk mitigation measures.[xvii]"

The AWWA has also published The Process Control System Security Guidance for the Water Sector, which highlights 12 cybersecurity "practice categories, and recommends specific critical practices under each category that direct map water-specific application to the NIST cybersecurity framework.[xviii]" Furthermore, the AWWA has designed an evaluative test, the Cyber Security Evaluation Tool (CSET) in order to assist water utilities companies in identifying the weaknesses within their virtual networks and systems. The CSET allows "a utility to compare their safeguards against a set of established standards, provided by NIST and other organizations," and "provides an output which includes a prioritized list of recommendations for improving the cybersecurity of the controls system.[xix]"

In addition to these frameworks, the Department of Homeland Security and the United States Environmental Protection Agency issued the Water and Wastewater Systems Sector-Specific Plan to address threats and vulnerabilities associated with drinking water and wastewater utilities, with goals to "sustain protection of public health and the environment," "recognize and reduce risk," "maintain a resilient infrastructure," and "increase communication outreach, and public confidence.[xx]" Efforts to achieve these goals include expanding resources to strengthen education and awareness of cyber risks, designing sustainable tools and guidance on cybersecurity, and bolstering communication from government personnel concerning threat information among water operating companies.

B: Federal and State Legislation

Regulation regarding cybersecurity in the water sector varies from state to state in terms of legislation. New Jersey, for example, enacted the Water Equality Accountability Act in 2017, establishing "new requirements designed to improve the safety, reliability and administrative oversight of the water infrastructure[xxi]" in all public water systems with greater than 500 service connections. The Act also institutes consistent maintenance, inspection, and updating of these companies' virtual assets. In the state of New York, public health law requires water suppliers and operators to design and establish emergency plans that include "'vulnerability analysis assessment, including an analysis of vulnerability to terrorist attack and cyber-attack, which shall be made after consultation with local and state law enforcement agencies.[xxii]'"

America's Water Infrastructure Act of 2018 provides federal legislation for community water systems servicing more than 3,300 individuals, establishing that they must conduct "a risk and resilience assessment of their systems," including testing security applications on any automated or virtual assets used.[xxiii] Additionally, on March 15, 2022 the Biden-Harris Administration passed the Cyber Incident Reporting for Critical Infrastructure Act in response to an increasing number of cyberattacks on critical infrastructure providers and "growing concerns of retaliatory cyberattacks relating to Russia's invasion of Ukraine.[xxiv]" This piece of legislation requires owners and operators of critical infrastructure to "report certain cyber incidents to the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Homeland Security within 72 hours," and "report ransomware payments within 24 hours.[xxv]"

Despite the advisory agencies, systems, legal protocols, and frameworks put into place to protect water infrastructure systems, recent history of cyberattacks have proven that they continue to be vulnerable to foreign intrusion.

IV: Types of Cyber Attacks and A History of Cyber Attacks on U.S. Water Infrastructure Systems

A: Types of Cyber Attacks

Over the past 20 years, the U.S. has faced an increasing number of cyber-attacks on their water infrastructure systems, highlighting the gravity and urgency of increasing its security. The Water and Wastewater Sector has endured a variety of attacks, ranging from "ransomware attacks, tampering with Industrial Control Systems, manipulating valve and flow operations and chemical treatment formulations, and other efforts to disrupt and potentially destroy operations.[xxvi]" Water and Wastewater facilities are vulnerable to "spearphishing personnel in order to deliver malicious payloads, including ransomware;[xxvii]" company employees may open "malicious attachments or links to execute malicious payloads contained in email from threat actors that have successfully bypassed email filtering controls.[xxviii]" Using this technique, hackers could gain the ability to exploit virtual services and control systems that allow for remote access and potentially control of water and wastewater networks. In addition to the use of ransomware, attackers may exploit "unsupported or outdated operating systems and software.[xxix]" Because water and wastewater facilities often prioritize the designation of resources to physical assets within their systems for maintenance or repair, IT/OT infrastructure is not always as sophisticated and updated as is necessary, opening an avenue for hackers to capitalize on. Likewise, water and wastewater systems "commonly use outdated control system devices of firmware versions, which expose WWS networks to publicly accessible and remotely executable vulnerabilities.[xxx]" Through the exploitation of these control systems, facilities may lose system control or sensitive data.

B: A History of Cyber Attacks on U.S. Water Infrastructure Systems

In 2006, "hackers planted a computer virus on the laptop computer of an employee" within Pennsylvania's water filtering plant stationed in Harrisburg, Pennsylvania. Using this virus, foreign hackers "installed malicious software on the plant's computer system.[xxxi]" While the attackers did not ultimately plan to exploit the water system itself, their access to the operating system could have allowed them to alter "the concentration levels of disinfectants in the potable water[xxxii]" and heavily disrupt the plant's operations.

In 2013, Iranian activists gained remote access to the SCADA system of Bowman Avenue Dam in Rye, New York, allowing them full access to "information on water levels, temperature, and the status of the sluice gate" of the dam.[xxxiii] The attackers employed a computer hacking technique called Google dorking, allowing them to leverage "the Google search engine to locate specific strings- and thereby vulnerabilities- in web applications," like the one responsible for controlling the sluice gate.[xxxiv] Although the gate was nonfunctional due to maintenance at the time of the attack, "remediation costs for the dam exceeded $30,000.[xxxv]"

In March of 2018, Atlanta suffered a ransomware attack, preventing employees of the Atlanta Department of Watershed Management from using their computers or networks for an entire week. After the attack, the city of Atlanta had to completely take down their water department website for redesign and construction. The city paid almost $5 million to recover from the attack.[xxxvi]

After Hurricane Florence in 2018, Onslow Water and Sewer Authority in Jacksonville, North Carolina suffered a ransomware attack, preventing company employees from accessing data and hindering their ability to provide water services to their customers.[xxxvii] Hackers used a virus known as EMOTET and were able to encrypt files and data within the authority's network.

In February of 2021, a group of hackers "attempted to poison the water supply" in Oldsmar, Florida by "increasing the amount of sodium hydroxide… in the water from 100 parts per million to 11,100 parts per million," which would have generated highly toxic drinking water for the treatment center's customers.[xxxviii] While the attack was prevented by operators that reversed the change promptly, it could have resulted in significant damage to public health.

During March of 2019, "a former employee at Kansas-based WWS facility unsuccessfully attempted to threaten drinking water safety by using his user credentials, which had not been revoked at the time of his resignation, to remotely access a facility computer.[xxxix]" He was charged with attempting to shut down the operator's cleaning and disinfecting processes through a remote login to the facility's computer system.

In 2014, government personnel in Flint, Michigan decided to switch the community's drinking water supply from Lake Huron to the Flint River. Lack of treatment and testing of this water resulted in intense water quality issues and contamination, "contributing to a doubling—and in some cases, tripling—of the incidence of elevated blood lead levels in the city's children, imperiling the health of its youngest generation.[xl]" Within a year, the toxic water caused an outbreak of Legionnaires' disease among the community, killing more than 13 people.[xli] While the crisis in Flint, Michigan was not caused by a cyberattack, the long term devastating felt by the Flint community demonstrates the colossal impact disruption in water systems can have to the health and well-being of American citizens. In fact, although the majority of the cyberattacks listed previously were detected before serious damage ensued, any one of them could have caused major economic and public health consequences.

It has become overwhelmingly clear that American water infrastructure systems are vulnerable to attacks that can have long-lasting, severe impacts on public safety and that these attacks are increasing in frequency as time continues. Tom Carper, Chairman of the U.S, Senate Committee on Environment and Public Works, "listed cyber-risk as the number one threat facing the U.S. water sector," and that "the Russian government was specifically targeting the water sector and other critical infrastructure as part of a multi-stage intrusion campaign.[xlii]" As the possibility of a cyber world war becomes increasingly probable, safeguarding American water supply is critical.

V: Water Sector Security Challenges

Challenges facing the water sector are physical, organizational, and technological.[xliii] Aside from cyber risk in the water sector, the system already faces a number of challenges including "infrastructure deterioration, large water losses, increasing pressures on the water resources with respect to both quality and quality," and as the population continues to grow exponentially, these issues will become more and more prominent.[xliv] As a result of these growing demands and pressures on the industry, optimization through digitalization of the water sector is becoming increasingly critical. However, a variety of issues have been identified regarding cybersecurity of the water sector.

A: Disintegration between cyber and physical assets

Despite the water sector infrastructure being composed of interconnected physical and cyber assets, security systems for each variety are completely disintegrated. In fact, "measures and approaches that consider a global integrated security context, physical and cyber, are missing and therefore leading to the inability to cope with combined cyber-physical attacks which are of major concern.[xlv]" A cyberattack may threaten the contamination, supply of water, output of pollutants etc. of a water operator, highlighting the need for a unified cyber-physical approach to security and risk management.

B: Lack of information sharing mechanisms

In addition to fragmentation between cyber and physical assets within the water sector, water utilities and IT operators lack strong communication and information sharing mechanisms that would allow them to inform one another on previous cyberattack events or prevention techniques. An efficient forum of communication would allow water sector companies to be cognizant of security incidents, prepare for similar events facing their own operations, and enhance their ability to protect their services. Not only would "providing updated information and advanced models by a central organization about case studies, attack categories, and potential impacts" strengthen water entities ability to handle cyber threats, but "such information can incentivize the private market to offer dedicated solutions" as well.[xlvi] In addition to a lack of information sharing at a national level, the water-cyber interface is weak as well. Although the Water Authority corresponds with Water Utilities, the National Cyber Directorate as well as technology providers do not have a strong relationship with the water sector, and lack a thorough understanding of the industry's operations.[xlvii]

C: Knowledge gap and lack of professional personnel

Furthermore, there appears to be an overarching knowledge gap concerning the implementation of cybersecurity in water systems among the industry. Although "knowledge about cybersecurity threats, procedures, and technologies is required by the organizations implementing cybersecurity, including their workers and supplies," "the water sector is composed of parties of different sizes, making it difficult for small organizations to employ dedicated personnel for cybersecurity.[xlviii]" Within the water sector, an overall lack of professional knowledge concerning cybersecurity presents a major challenge for its operations safety.

As cybersecurity in the water sector is relatively novel, "there is a lack of dedicated professional personnel in the market," and recruiting trained professionals and staff poses a large economic cost on industry operators.[xlix] Likewise, technology systems within the water sector are rapidly evolving, as the industry as a whole undergoes a process of digitization and day to day operations becoming increasingly virtual, contributing to the challenge of proper professional education and personnel.

VI: Recent Change to Bolster Cybersecurity in the Water Sector

On January 27, 2022, the Biden-Harris Administration declared its intention to "extend the Industrial Control Systems Cybersecurity Initiative to the water sector.[l]" With a goal of improving cybersecurity within the water sector, the Biden-Harris Administration, Environmental Protection Agency (EPA), Cybersecurity and Infrastructure Security Agency (CISA), and the Water Sector Coordinating Council (WSCC) designed the Water Sector Action Plan to "facilitate the deployment of technologies and systems that provide cyber-related threat visibility, indicators, detections, and warnings.[li]" Like previous action plans within electric and pipeline critical infrastructure systems, the Water Sector Action Plan will help providers implement technology that will "monitor their systems and provide near real-time situational awareness and warnings," as well as facilitate communication regarding cybersecurity information between the government and other stakeholders in the industry.[lii] The Plan also asserts that the Environmental Protection Agency and the Cybersecurity and Infrastructure Security Agency will collaborate with water utilities and conduct pilot programs for Industrial Control Systems "monitoring and information sharing." Because the sector includes a multitude of systems from small to spanning country-wide and public to private, the EPA and CISA will dedicate efforts and resources to private partners, designing strong protocol for communication, information sharing, and data analysis among the thousands of water sector companies within the United States.

VII: Changes to be Made to Strengthen Cybersecurity in the Water Sector

A: Creation of a national research and development center

While the Biden-Harris Administration's declaration of the Water Sector Action Plan represents growth in strengthening cybersecurity within the water sector, additional changes must be made to bolster cyber resilience in the U.S. water industry. In order to address the lack of professional knowledge regarding cybersecurity in the water sector, standardized systems setting a threshold for professional qualifications is imperative. Specifically, "Water Utilities and the Water Authority should define precise specifications for employees and raise salaries for such professional positions.[liii]" Such personnel "should also be responsible for developing cybersecurity guidelines, including systems documentation and risk surveys, and implement routine exercises, simulations, and conference participation with the support and funding from the Government, including the National Cyber Directorate.[liv]" In order to facilitate these efforts, the creation of a national research and development center within the Water Authority would be extremely beneficial. Additionally, "the Government and the Water Authority should increase cybersecurity positions and raise salaries to attract skilled IT personnel to the water sector.[lv]"

B: Establishment of round tables and group forums

To target the lack of information sharing concerning cybersecurity in the water sector, water infrastructure companies could work with the National Cyber Directorate to form "a cyber forum and security operations center," and endorse an effective, accessible information sharing mechanism.[lvi] In order to strengthen the water-cyber interface, the Water Authority and National Cyber Directorate could assemble round tables and group discussions and exercises, so that each party "would better understand the needs and obstacles for cybersecurity implementation, and Water Utilities would enhance their capabilities and be exposed to the support and funding provided by the Government.[lvii]"

C: Institution of public-private partnerships

As the design, creation, and implementation of strong cybersecurity systems and practices can be extremely expensive for water utility companies, which are profit-based, often private organizations, these companies should emphasize "the crucial importance of implementing cybersecurity by dedicated public relations campaigns," and with the public's support, the Government should include "cybersecurity expenses within the water tariff.[lviii]"

Constantly revising technology within cybersecurity systems serves as a significant upfront cost for many water utilities companies. While the Drinking Water and Wastewater Infrastructure Act of 2021, a bill that would authorize "the appropriation of grants for improving the cybersecurity of water treatment facilities[lix]" represents a step in the right direction in regards to federal economic support to cybersecurity within the water sector, establishing public-private partnerships with government entities may be even more beneficial for overcoming significant financial barriers.

D: Federally-mandated standards and protocols

A study investigating viable improvements to cybersecurity within the water sector establishes "a new sector-led organization to manage the development of mandatory cybersecurity standards and oversee compliance with them.[lx]" Using the Environmental Protection Agency as the primary Federal oversight and enforcement agency, mandatory standards providing "a much needed 'floor' for cyber resilience" would be established.[lxi] In order to implement this new and improved set of standards for cybersecurity in water systems, building on existing frameworks would be most beneficial; "for water systems, that foundation includes the National Institute of Standards and Technology (NIST) Cybersecurity Framework and section 2013 of America's Water Infrastructure Act of 2018 (AWIA).[lxii]" Because the Environmental Protection Agency and the Water Information Sharing and Analysis Center also provide recommendations for cybersecurity in the water and wastewater utilities sector, using these guidelines, as well as the ones mentioned before, to design a mandatory protocol would be most efficient.

E: Collaboration between enforcement organizations and industry professionals

In order to ensure these government-imposed mandatory standards reflect thorough understanding of the specificities of the water industry, a system modeled after the Bulk Power System's regulatory process could be established. With the Bulk Power System, "the North American Electric Reliability Corporation (NERC) – work to develop standards that are vetted and then either approved or, on rare occasions, rejected by the Federal Electricity Regulatory Commission (FERC). FERC serves the federal oversight function, while NERC develops and assesses compliance with approved standards.[lxiii]" Because the sector itself assists in creating compliance standards, Bulk Power System companies will be more likely to "be supportive of the enforcement system that 'holds the stick' over them to create accountability.[lxiv]" Modeled after Bulk Power System's process of regulation and enforcement, this study suggests the development of a new entity, the Water Risk & Resilience Organization (WRRO) "to lead the development of mandatory standards, with strong participation by water sector representatives.[lxv]" Either a "water sector counterpart to FERC" or the Environmental Protection Agency could provide governmental oversight and federal enforcement of these standards.[lxvi]

VII: Conclusion

As the fifth industrial revolution quickly approaches, and our world becomes more and more dependent on Artificial Intelligence, Big Data, the Internet of Things, and digital platforms, protecting cyber assets within water infrastructure systems in the United States becomes increasingly integral to the safety of our citizens, our economy, and a functioning society. Through the creation of a national research and development center to bolster professional knowledge within the industry, an assembly of round tables and group discussions to facilitate information sharing, the establishment of public-private partnerships to overcome financial challenges, the institution of federally-mandated standards for water utilities companies, and collaboration between regulatory agencies and the water sector, the United States will be better prepared to mitigate future cyberattacks and safeguard its citizens. The Russia Ukraine conflict serves as a frightening example of the transformation from physical to cyber warfare in modern day, and the calamitous impact cyberattacks can have. Within the past few months, Russian hackers have infiltrated Ukrainian government and banking systems and within the past few weeks has attempted to attack Ukraine's energy infrastructure. The onslaught of cyberattacks on Ukraine demonstrate that a cyberwar between Russia and the West is very much so possible, and the consequences of such could be far worse than any "traditional" war the world has seen before. Whether it is a singular foreign cyberattack or a full blown cyber-based third World War, virtual ambushes on our critical infrastructure systems are inevitable, and protecting them is a matter of national priority.

Endnotes

[i] Soldatos, John, James Philpot, and Gabriele Giunta. *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Hanover, MA: now, 2020.

[ii] Morrison, Sara. "Ransomware Attack Hits Another Massive, Crucial Industry: Meat." Vox. Vox, June 1, 2021. https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers.

[iii] Hassanzadeh, Amin, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M. Katherine Banks. "A Review of Cybersecurity Incidents in the Water Sector: Journal of Environmental Engineering: Vol 146, No 5." Journal of Environmental Engineering. American Society of Civil Engineers, February 28, 2020. https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29EE.1943-7870.0001686?casa_token=h1wrnwwp4cUAAAAA%3AaEmf_UuidIQAYqbCaSJfqCRNYfPvH7fW7Xp3gYiIXaRVeJg8SeHP7WlwbqUrcQaFCiA4yU-tZA.

[iv] "Water and Wastewater Systems Sector." Cybersecurity and Infrastructure Security Agency CISA. Accessed April 25, 2022. https://www.cisa.gov/water-and-wastewater-systems-sector.

[v] Copeland, Claudia. "Terrorism and Security Issues Facing the Water Infrastructure Sector," December 15, 2010. https://sgp.fas.org/crs/terror/RL32189.pdf.

[vi] *Id*

[vii] "Understanding America's Water and Wastewater Challenges." Bipartisan Policy, May 2017. https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/BPC-Infrastructure-Understanding-Americas-Water-and-Wastewater-Challenges.pdf.

[viii] Rao, Vikram M., and Royce A. Francis. 2015. Critical review of cybersecurity protection procedures and practice in water distribution systems. *IIE Annual Conference.Proceedings*: 2019-2028, https://login.proxy.lib.duke.edu/login?url=https://www.proquest.com/scholarly-journals/critical-review-cybersecurity-protection/docview/1792030538/se-2?accountid=10598 (accessed April 25, 2022).

[ix] "Improved Water & Wastewater Systems Monitoring and Automation with SCADA." Alliance Water Resources, January 20, 2021. https://alliancewater.com/how-does-scada-help-water-and-wastewater-management/.

[x] "Water and Wastewater Sector-Specific Plan - 2015 - CISA." Accessed April 26, 2022. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.

[xi] "Ongoing Cyber Threats to U.S. Water and Wastewater Systems." CISA, October 25, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-287a.

[xii] Rao, Vikram M., and Royce A. Francis. 2015. Critical review of cybersecurity protection procedures and practice in water distribution systems. *IIE Annual Conference.Proceedings*: 2019-2028, https://login.proxy.lib.duke.edu/login?url=https://www.proquest.com/scholarly-journals/critical-review-cybersecurity-protection/docview/1792030538/se-2?accountid=10598 (accessed April 25, 2022).

[xiii] *Id*

[xiv] Germano, Judith H. "Cybersecurity Risk & Responsibility in the Water Sector." American Water Works Association, 2019. https://www.waterisac.org/system/files/articles/AWWACybersecurityRiskandResponsibility.pdf.

[xv] *Id*

[xvi] *Id*

[xvii] *Id*

[xviii] *Id*

[xix] *Id*

[xx] "Water and Wastewater Sector-Specific Plan - 2015 - CISA." Accessed April 26, 2022. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.

[xxi] Germano, Judith H. "Cybersecurity Risk & Responsibility in the Water Sector." American Water Works Association, 2019. https://www.waterisac.org/system/files/articles/AWWACybersecurityRiskandResponsibility.pdf.

[xxii] *Id*

[xxiii] *Id*

[xxiv] "President Biden Signs into Law the Cyber Incident Reporting for Critical Infrastructure Act, Expanding Cyber Reporting Obligations for a Wide Range of Public and Private Entities." Gibson Dunn, March 22, 2022. https://www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/.

[xxv] *Id*

[xxvi] Germano, Judith H. “Cybersecurity Risk & Responsibility in the Water Sector.” American Water Works Association, 2019. https://www.waterisac.org/system/files/articles/AWWACybersecurityRiskandResponsibility.pdf.

[xxvii] “Ongoing Cyber Threats to U.S. Water and Wastewater Systems.” CISA, October 25, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-287a.

[xxviii] *Id*

[xxix] *Id*

[xxx] *Id*

[xxxi] Hassanzadeh, Amin, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M. Katherine Banks. “A Review of Cybersecurity Incidents in the Water Sector: Journal of Environmental Engineering: Vol 146, No 5.” Journal of Environmental Engineering. American Society of Civil Engineers, February 28, 2020. https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29EE.1943-7870.0001686?casa_token=h1wrnwwp4cUAAAAA%3AaEmf_UuidIQAYqbCaSJfqCRNYfPvH7fW7Xp3gYiIXaRVeJg8SeHP7WlwbqUrcQaFCiA4yU-tZA.

[xxxii] *Id*

[xxxiii] *Id*

[xxxiv] *Id*

[xxxv] Germano, Judith H. “Cybersecurity Risk & Responsibility in the Water Sector.” American Water Works Association, 2019. https://www.waterisac.org/system/files/articles/AWWACybersecurityRiskandResponsibility.pdf.

[xxxvi] *Id*

[xxxvii] Hassanzadeh, Amin, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M. Katherine Banks. “A Review of Cybersecurity Incidents in the Water Sector: Journal of Environmental Engineering: Vol 146, No 5.” Journal of Environmental Engineering. American Society of Civil Engineers, February 28, 2020. https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29EE.1943-7870.0001686?casa_token=h1wrnwwp4cUAAAAA%3AaEmf_UuidIQAYqbCaSJfqCRNYfPvH7fW7Xp3gYiIXaRVeJg8SeHP7WlwbqUrcQaFCiA4yU-tZA.

[xxxviii] Magill, Jim. “U.S. Water Supply System Being Targeted by Cybercriminals.” Forbes. Forbes Magazine, July 26, 2021. https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals/?sh=7415c65e28e7.

[xxxix] “Ongoing Cyber Threats to U.S. Water and Wastewater Systems.” CISA, October 25, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-287a.

[xl] Denchak, Melissa. “Flint Water Crisis: Everything You Need to Know.” NRDC, October 26, 2021. https://www.nrdc.org/stories/flint-water-crisis-everything-you-need-know.

[xli] Lane, Madeleine, James Polidori, and Sara Hughes. “The Flint Water Crisis : Could the Flint Water Crisis Happen Somewhere Else?” Gala. Accessed April 25, 2022. https://www.learngala.com/cases/flint-water-crisis/2.

[xlii] Magill, Jim. “U.S. Water Supply System Being Targeted by Cybercriminals.” Forbes. Forbes Magazine, July 26, 2021. https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals/?sh=7415c65e28e7.

[xliii] Germano, Judith H. “Cybersecurity Risk & Responsibility in the Water Sector.” American Water Works Association, 2019. https://www.waterisac.org/system/files/articles/AWWACybersecurityRiskandResponsibility.pdf.

[xliv] Soldatos, John, James Philpot, and Gabriele Giunta. *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Hanover, MA: now, 2020.

[xlv] *Id*

[xlvi] Shapira, Naama, Ofira Ayalon, Avi Ostfeld, Yair Farber, and Mashor Housh. “Cybersecurity in Water Sector: Stakeholders Perspective: Journal of Water Resources Planning and Management: Vol 147, No 8.” Journal of Water Resources Planning and Management. American Society of Civil Engineers, May 18, 2021. https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29WR.1943-5452.0001400?casa_token=ECoPYYY_vXIAAAAA%3AKDi4mwYfb7WQOY0gPFaRD0-FoGn6wl1S01lhrm6S2CdOqz_L-yZfnjDnlUE-430xQl47iB3aVQ.

[xlvii] *Id*

[xlviii] *Id*

[xlix] *Id*

[l] “Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector.” The White House. The United States Government, January 27, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/.

[li] *Id*

[lii] *Id*

[liii] Shapira, Naama, Ofira Ayalon, Avi Ostfeld, Yair Farber, and Mashor Housh. “Cybersecurity in Water Sector: Stakeholders Perspective: Journal of Water Resources Planning and Management: Vol 147, No 8.” Journal of Water Resources Planning and Management. American Society of Civil Engineers, May 18, 2021. https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%29WR.1943-5452.0001400?casa_token=ECoPYYY_vXIAAAAA%3AKDi4mwYfb7WQOY0gPFaRD0-FoGn6wl1S01lhrm6S2CdOqz_L-yZfnjDnlUE-430xQl47iB3aVQ.

[liv] *Id*

[lv] *Id*

[lvi] *Id*

[lvii] *Id*

[lviii] *Id*

[lix]Baksh, Mariam. “White House Endorses Inclusion of Cybersecurity in Water Infrastructure Bill .” Nextgov.com. Nextgov, April 28, 2021. https://www.nextgov.com/cybersecurity/2021/04/white-house-endorses-inclusion-cybersecurity-water-infrastructure-bill/173678/.

[lx] Stockton, Paul N. “STRENGTHENING THE CYBERRESILIENCE OF AMERICA’S WATER SYSTEMS: INDUSTRY-LED REGULATORY OPTIONS.” *American Water Works Association*, August 27, 2021.

[lxi] *Id*

[lxii] *Id*

[lxiii] *Id*

[lxiv] *Id*

[lxv] *Id*

[lxvi] *Id*