SECURING OPERATIONAL TECHNOLOGY:

A DEEP DIVE INTO THE WATER SECTOR

HEARING
BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION
ONE HUNDRED EIGHTEENTH CONGRESS

_____

6 FEBRUARY 2024, CANNON HOUSE OFFICE BUILDING

_____

Robert M. Lee

Chairman Garbarino, Ranking Member Swalwell and distinguished members of the Subcommittee, thank you for providing me the opportunity to testify before you today. My name is Robert M. Lee and I am the CEO and Co-Founder of Dragos, Inc. a leading industrial cybersecurity technology and services provider. Additionally, I serve in advisory roles to numerous governments and international organizations across the world including the United States Department of Energy (DOE), Singapore's Cyber Security Agency, and the World Economic Forum's cybersecurity committees on oil and gas and electricity. I am a veteran of the United States Air Force and National Security Agency. It has been my privilege to be on the front lines of this problem in both government and the private sector.

Both government and industry have invested significantly in the cybersecurity of our nation's critical infrastructure. However, a vast majority of the focus has been on securing information technology (IT) networks. Less emphasis was traditionally placed on cybersecurity for operational technology (OT) and industrial control systems (ICS). These systems are the specialized computers and networks that interact with the physical world, including assets like a control system that opens a circuit breaker on an electric substation or operates pumps at a water facility. Most executives and policy leaders are shocked to find that upwards of 95% of cybersecurity budgets go to the Enterprise IT portions of the business and not the OT networks that can impact safety, the environment, and generate the revenue for the organization. OT systems are the critical part of critical infrastructure.

Even twenty years ago, ICS and OT were largely disconnected from other networks. The infrastructure was also complex and heterogenous with little in common between two facilities even in the same industry, making it more difficult and more costly for adversaries to create attacks that caused disruption or physical destruction in a way that was repeatable across sites and industries. Now, these systems, including those in the water and wastewater sector, are increasingly digital and homogenous by necessity. Threat groups can develop capabilities that target devices commonly used in OT environments

across sectors and have found new ways to access and manipulate them causing disruption and posing safety risks.

In 2018, I testified before Congress that Dragos, Inc. tracked five state actor cyber groups that targeted industrial networks specifically. At the time, I noted that while that sounded alarming, we had time to address these issues if we worked diligently. Today, Dragos tracks over 20 such groups and my message has more urgency. Water utilities and other critical infrastructure organizations are also facing challenges stemming from the current geopolitical environment. They find themselves on the front lines, often with very limited resources, needing to defend against both state actor cyber groups and criminal groups.

To protect and defend OT in the water sector requires both an understanding of the environment and investment in the right resources. My testimony focuses on three key points that are relevant to the Subcommittee and this hearing's focus.

- The first point is that there are fundamental differences between the operational technology and information technology that underpin our nation's critical infrastructure. IT is focused on how you enable and manage the business while OT is focused on why you are a business. The different missions, or purposes, of IT and OT systems dictate what is required of them and how organizations manage risk to them. The risks and threats to those systems, how the threats operate, the consequence of attacks, as well as the controls used to manage that risk, are also different across OT and IT environments.

- The second point is that the cyber threat landscape for operational technology and industrial control systems, including those used in facilities in the water and wastewater sector, has shifted irreversibly in recent years. The same digitalization, connectivity and uniformity in OT that is enhancing efficiency and reliability for infrastructure owners and operators is also adding risk. This digital transformation of our industrial industries is necessary but without investing in cybersecurity in advance of that transformation the consequences will be dire. To minimize that risk and defend water systems and other infrastructure against those adversaries, the community must invest in and prioritize the cybersecurity of OT and ICS networks with a focus on implementing security controls that have demonstrated success against the methods used by those threat groups.

- The third point is that the public and private sectors must continue to work together to make sure infrastructure owners and operators, including small and under-resourced organizations, have the information, tools and resources they need to protect their systems. Both government and industry have unique capabilities and insights that provide real value to operators of infrastructure, including water and wastewater systems. We need to remove barriers that those operators face in accessing information, tools and equipment they need to defend their systems. We must also not forget that the issues are primarily an economics and awareness issue at our numerous municipally owned water utilities across this country. No amount of free vendor tools or tax payer funded cybersecurity services will alleviate this issue without addressing the core economic challenge.

I. IT and OT Are Fundamentally Different

Both conceptually and functionally, IT and OT are fundamentally different. The biggest difference between IT and OT is the mission or business purpose of the system. Generally, IT systems are designed to support how you manage business. OT systems focus on the reason the business or organization exists. OT systems are the specialized computers and networks that interact with the physical environment to do things like control the pumps or chemical levels at a water treatment facility.

The distinct mission, or purpose, of those systems dictates what is required of them and informs how risks and threats to the system are defined and managed. For example, a Windows operating system computer hosting a database for a financial institution has a distinctly different purpose and impact of failure than a Windows operating system hosting the Human Machine Interface (HMI) for a nuclear power plant. An adversary may be able to exploit a targeted Windows system in a similar way across IT and OT, but their behavior within that system will differ depending on whether they are focused on intellectual property theft of the financial institution's database or on causing an unsafe operating condition and physical impact.[1]

The impact of a breach or compromise is different as well. IT tends to be focused on system and data security, and OT tends to focus on the system of systems and physics. In many IT compromises, gaining access to the system and understanding the system or its data are critical. The goal is likely data theft or disabling the systems. The adversary, in this case, does not often seek to cause physical impacts. In the OT cybersecurity community, the types of attacks that cause the greatest concern are those that seek to disrupt operations, cause physical damage, or even cause safety-related incidents that lead to equipment damage or loss of life. The threats operate differently, often using unique methods and capabilities to achieve their goals in OT networks.

OT also has unique requirements. While the requirements of both IT and OT environments sound similar– high uptime, redundancy, low latency – OT must support specific circumstances. High uptime for OT, for instance, is often measured in years, not months, with systems that literally run for multiple years between rounds of maintenance. Redundancy for OT focuses on availability more than security. Many OT critical components can't be turned off. Instead of the time it takes to move data from one place to another, latency in OT deals with the milliseconds that determine whether an assembly line functions correctly.

OT security requires a different mentality. It is unique from IT security. This is due to the nature of the physical environments and also because the threats that target them are different. The way threat groups operate, as well as the tactics and techniques they use, are different across IT and OT environments. Even just a decade ago, the threat landscape for operational technology (OT) and industrial control systems (ICS) was very limited. As a result, many of the security controls for OT have traditionally been IT controls that can be applied to OT environments. Many standards, regulations, and "best practices" are often focused on how to apply IT security controls to OT and not whether they should be applied. There are many IT cybersecurity practices, such as vulnerability management and

[1] https://www.sans.org/white-papers/36297/

endpoint protection systems, that have a completely different value proposition, emphasis, and effect in OT networks. Applying all of the IT cybersecurity controls of a business to the OT networks would yield wasted resources and likely cause more disruption to the environment than all the state actors currently tracked combined. Simply put, organizations should look to unique OT cybersecurity controls and then evaluate the IT cybersecurity controls based on what risk they reduce and, if so, the unique way they should be applied. Our communities cannot afford for companies to "gold plate" the problem nor can they afford them to ignore it.

II. The Cyber Threat Landscape for OT Has Shifted Irreversibly

Increasing digitalization, connectivity, and homogeneity in OT is changing the threat landscape

The same digitalization, connectivity, and uniformity in OT that is enhancing efficiency and reliability for infrastructure owners and operators is also adding risk. At the same time, a growing number of threat groups are targeting OT. To minimize that risk and defend water systems and other infrastructure against those adversaries, the community must invest in and prioritize the cybersecurity of OT and ICS networks with a focus on implementing security controls that have demonstrated success against the methods used by those threat groups.

Twenty years ago, manual and truly disconnected OT environments meant that cyber adversaries could not as easily reach or interact with OT systems through cyber means. However, as those environments started becoming connected and digitalized, adversaries have paid attention. In 2015 and 2016 Ukraine experienced the first power outages due to cyber attacks that used malicious software, or malware, that could be deployed at other electric transmission substations around the world. In 2017 the first ever cyber attack that targeted human life directly took place in a Saudi Arabian petrochemical facility by targeting an OT safety system.

As industry has moved towards more homogenous infrastructure with common software packages, common network protocols and common facility designs, it has brought both cost and operating efficiencies. At the same time, it has also reduced the complexity in which adversaries have to operate and opened the door for reusable, scalable adversary capabilities that can be used to target the OT of multiple organizations within and across sectors. Threat groups are also taking advantage of native functionality in increasingly digitalized and connected systems, demanding an emphasis on detection and response efforts, in addition to prevention.

In 2022, Dragos and its third-party partner in collaboration with the U.S. government discovered and analyzed PIPEDREAM, the first reusable cross-industry capability that can cause physical disruption or destruction. The PIPEDREAM toolkit has the capabilities to impact devices that control critical infrastructure in different sectors – devices that manage electrical systems, oil and gas pipelines, water systems, manufacturing plants, and even the control systems in military assets such as unmanned aerial vehicles and naval ships. PIPEDREAM also cannot simply be patched away as it takes advantage of native functionality in the software and network protocols available cross-industry. Prevention is important to attempt but the necessity is on identifying, detecting, responding, and recovering correctly. At best guess

currently less than 5% of global infrastructure has the ability to achieve this against PIPEDREAM-like capabilities.

Though a capability like PIPEDREAM is concerning, it is important to take a moment to acknowledge the victory here as well. Dragos and its partners worked with federal agencies to identify, analyze, and report on PIPEDREAM to the broader infrastructure community prior to PIPEDREAM being employed. This is one of the most significant public-private partnership wins of all time in cybersecurity and truly represents a "left of boom" moment for the industry. The capability can still be used in the future though and it would be shocking if other countries were not developing similar capabilities.

Threats to water and wastewater systems have the potential to disrupt operations and pose safety risks

Water and wastewater systems are vulnerable to a variety of cyber attacks that have the potential to disrupt operations and pose safety risks to the systems' ability to perform fundamental functions. In over half of our engagements with customers, Dragos has encountered issues with ICS/OT network accessibility from the internet.[2] Using weak or default credentials, which are often publicly available in the vendor's documentation, for OT devices increases the threat of exposure. Several recent examples demonstrate adversaries exploiting ICS/OT exposed systems.

- In November 2023, CyberAv3ngers, a self-styled hacktivist collective, executed an exploitation campaign targeting Unitronics programmable logic controllers (PLCs) across multiple sectors, including the water and wastewater sector. The campaign employed unsophisticated methods such as secure shell (SSH) brute-forcing and exploiting default configurations.[3] In December 2023, government agencies from the United States and Israel released a joint Cybersecurity Advisory linking the activity to Iranian National Revolutionary Guard (IRGC) activities targeting an Israeli company.[4] The campaign's impact was notable, causing operational disruptions such as the shutdown of a water scheme in North Mayo, Ireland, and affecting wastewater treatment facilities in the U.S. Despite the unsophisticated nature of the attacks, they underscored the potential for high-impact consequences in industrial control systems (ICS) environments, highlighting the disparity between attack sophistication and potential operational impact. This also emphasizes the urgent need for organizations with OT environments to implement fundamental security measures, adhere to critical controls, and conduct regular monitoring to mitigate risks.

- In January 2021**,** an adversary used stolen TeamViewer credentials to delete programs related to the water treatment system for a San Francisco water utility.[5] Dragos is unaware whether the deleted water treatment programs were in an ICS/OT system, but had the attack been

[2] https://www.dragos.com/year-in-review/
[3] https://www.dragos.com/blog/cyber-av3ngers-hacktivist-group-targeting-israel-made-ot-devices/
[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
[5] https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

successful, San Francisco's water operations certainly would have been impacted through loss of control, availability, and safety.

- In February 2021, similar to the attack against the San Francisco water treatment facility, an adversary leveraged stolen TeamViewer credentials to access a human-machine interface (HMI) in the ICS/OT environment of an Oldsmar, Florida, water supply organization to change the water's sodium hydroxide (NaOH) level.[6] If successful, the Oldsmar water supply would have been poisoned and may have impacted the health of Oldsmar's citizens. The similarity of the San Francisco and Oldsmar attacks, including the same initial intrusion techniques, highlights how universal OT architecture within the water and wastewater sector can lower the barrier for adversaries to attack. Successful tactics, techniques and procedures (TTPs) used against one entity can be effective against others as well.

Adversaries are also targeting remote service technologies and solutions, as well as communications protocols. In 2023, Dragos observed an uptick in the water and wastewater sector in adversary actions using these types of connectivity. This highlights the importance of properly securing remote service applications and coordinating with third party vendors and contractors to do the same.

- In October 2021, in a joint advisory, the U.S. Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) stated that between 2019 and 2021, adversaries gained access to water and wastewater sector ICS/OT environments through spearphishing as an initial intrusion and then pivoting to ICS/OT environments through internet-accessible PLCs that required no authentication using remote services.[7]

- In January 2024, CyberArmyofRussia_Reborn, a known hacktivist group that has been associated with a known state actor, posted a video to their Telegram channel showing the manipulation of water tanks associated with two water authorities in Texas in the United States. Based on information in the video, it appeared that they changed the tank water level indicators, which turned on the pumps. The adversary remotely accessed the human-machine interface (HMI) via remote services, likely causing Damage to Property, Denial of Control, Manipulation of Control, and Loss of Availability.

Also notable, almost all of the activity observed by Dragos in the water and wastewater sector was indicative of reconnaissance efforts, suggesting adversaries are using tools to map out water entities' public-facing internet infrastructure for future operations.

While largely opportunistic, ransomware operators are increasingly attacking industrial organizations in several sectors, including water and wastewater. Ransomware has primarily threatened organizations' IT systems, without proper network hygiene, the connectivity between the IT and ICS/OT environments often provides a pathway for adversaries to attack ICS/OT systems directly. Double extortion tactics used

[6] https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/
[7] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

by ransomware operators add to the threat for water and wastewater organizations because releasing sensitive ICS/OT data and diagrams could provide other capable adversaries with valuable information they can use in campaigns with ICS/OT disruptive or destructive objectives.

- In August 2022, adversaries attacked a United Kingdom (UK) water supply company, South Staffordshire Water (SSW), using the cl0p ransomware. The ransomware operators disrupted SSW's corporate Information Technology (IT) network; however, their ability to supply clean public water was not impacted. On 16 August 2022, the ransomware operators posted pictures on its leak site of what appear to be stolen identification documents and screenshots of SSW's Human Machine Interfaces (HMIs). They claimed to have gained access to SSW's ICS/OT network and could manipulate chemical processes.[8]

III. The Public and Private Sectors Must Work Together to Make Sure Infrastructure Owners and Operators Have the Information, Tools, and Resources They Need to Protect Their Systems and Communities

The best way to help the water and wastewater sector, as well as other critical infrastructure sectors, protect against threats to their OT environments and to manage risk is for government and industry to work together, each using our unique capabilities, insights and expertise to provide real value to operators. We need to remove barriers that those operators face in accessing information, tools and equipment they need to defend their systems.

For federal agencies, such as CISA and EPA, this means focusing efforts at the strategic level, providing direction to industry regarding what to focus on protecting (i.e. what is a critically important entity/asset), what scenarios to protect against (such as the known threat scenarios to OT water systems), and provide opportunities to practice efforts while sharing knowledge. It also means investing in areas where the private sector isn't already investing and providing guidance that must come from the government. As an example, the Department of Energy's Cyber-Informed Engineering operates in an area where there is no market. It is intended to build cybersecurity resilience and principles into engineering efforts so that some of the cyber risks that we are concerned about are engineered out at a control and physics level before adversaries can exploit them. On the other hand, government resources continue to get funneled into grant programs and government initiatives that completely replicate technologies and services already available in the private sector that have been developed at lower costs with more expertise.

When it comes to regulation, the government must define and communicate what it is seeking to accomplish and prioritize outcomes. Dictating highly prescriptive controls that tell infrastructure owners how to run security in their own environments, which they know better than the government, will not reduce risk and is often counterproductive. I would recommend, instead, that the government coordinate with the private sector to use their expertise and knowledge of their systems to inform outcome-based regulations. Regulations should also be informed by research such as the SANS Institute's

[8] https://thecyberwire.com/newsletters/control-loop/1/4

5 ICS Cybersecurity Critical Controls[9], which analyzed all known cyber threat attacks to industrial systems and identified the most effective and efficient controls against them.

We have seen this work well with models that the Federal Energy Regulatory Commission (FERC) and North American Energy Reliability Corporation (NERC) use. A regulatory agency proposes a regulation with details on what it seeks to achieve. NERC then forms a committee of members across the community to evaluate the effectiveness and feasibility of the proposed changes. This allows time for input and alignment and creates regulations that better meet the objectives. Further, models for collaboration instead of simply information sharing have begun to show value. NERC also facilities GridEx, a valuable sector-wide, large scale operational exercise that brings government, vendors, and operators together under blue sky conditions to simulate real-world scenarios. The exercise provides real, valuable insights that inform future priorities.

Another example of government successfully providing this strategic level of direction is when the Administration reached out to the Electricity Subsector Coordinating Council, the industry-CEO led group that collaborates with CISA and DOE, to coordinate on its priorities on threats to electricity ICS and OT. The Administration essentially laid out ***why*** they were concerned, including insights to cyber threats, ***what*** outcome was necessary to detect and respond to such ICS/OT cyber threats, but left the ***how*** to the private sector. The CEOs led a group to rapidly enhance the visibility across our industrial networks in the sector to detect industrial cyber threats by deploying commercial technologies, including one developed by Dragos called Neighborhood Keeper. The result is that the United States government now voluntarily receives real time insights from across the ICS and OT networks of the power companies that serve over 70% of Americans for free and at any time can identify new cyber threats and vulnerabilities.[10] This model of **why,** and **what**, but not **how** allows for the government to set and communicate straightforward priorities while allowing the expertise and innovation of the infrastructure operators to advise on how best to achieve the desired outcomes.

In another example of successful public-private sector collaboration, Dragos worked with Rockwell Automation and the U.S. government in advance of the disclosure of a novel exploit capability attributed to a state actor that affected select communication modules by Rockwell Automation deployed in industrial companies across the country. The U.S. government was able to leverage the insights from Neighborhood Keeper to determine how far wide these assets and vulnerabilities could be found, work with Dragos and Rockwell to develop detections and mitigations, deploy them in real time to the asset owners in the Neighborhood Keeper network, and simultaneously make the insights available to those who were not.[11] Another great “left of boom” example of what right can look like when the public and private sector utilize their strengths.

When the government speaks with one voice, the infrastructure community listens. However, when owners and operators receive different priorities and guidance from different agencies, it can cause analysis paralysis in security teams. Agencies like CISA and EPA have tremendous opportunity to help

[9] https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
[10] https://www.utilitydive.com/news/an-eye-for-an-eye-the-electric-sectors-defense-will-depend-on-federal-g/601643/
[11] https://www.dragos.com/blog/mitigating-cves-impacting-rockwell-automation-controllogix-firmware/

critical infrastructure organizations prioritize security efforts to ensure they are investing in the things that truly reduce risk. For small organizations, like many water utilities, clear, relevant and aligned guidance really matters because they do not have large teams to analyze and prioritize recommendations.

Additionally, these efforts need to be properly resourced, both in the private sector and in the government. Some organizations have the resources and mechanisms to invest in cybersecurity. Many do not. There are thousands of water utilities across the country that share information technology contractors with other organizations simply to do basic information technology support. They do not have the expertise or resources for cybersecurity efforts, including those to protect operational technology. Free government assessments or further government investments in trying to develop the next greatest technology acutely miss their need. These smaller municipal and public utility infrastructure sites need direct resourcing through changes at a state and local level or resourcing from a federal level to go out and hire talent and purchase proven tools and technologies. Though we know "what" to do, the unfortunate reality is it is absolutely an economics issue.

In my role at Dragos, I see the challenges that these organizations face every day in building their OT cybersecurity programs. And so, in December, Dragos expanded our Community Defense Program to give under-resourced U.S.-based utility providers with under $100M in annual revenue free access, forever, to Dragos products and training to build their operational technology cybersecurity programs, improve their security posture, and reduce operational technology cyber risk. And yet, even with access to tens of thousands of dollars' worth of free technology and training each year most water sites will be unable to take advantage of the program. To use any technologies most of the water municipalities need basic infrastructure upgrades. Even a one-time cost of $3,000 on hardware and networking gear would be completely out of budget for these organizations and require a city council vote on the topic of cybersecurity that they do not likely understand. I have so much optimism about what we all can do together by playing to our strengths and caring enough about our communities to act using our knowledge to counter even the most sophisticated cyber threats. However, a major shift must take place in order for us to solve the underlying economic issues that would make any of it work at scale, especially in the water sector.

I. Conclusion

In conclusion, in order to help secure operational technology in the water sector, we must first understand the fundamental differences between the operational technology and information technology. The risks and threats to those systems, as well as the controls used to manage that risk, are also different across OT and IT environments. The cyber threat landscape for the OT environment has also shifted irreversibly. The same digitalization, connectivity and uniformity in OT that is enhancing efficiency and reliability for infrastructure owners and operators is also adding risk. To adequately defend water systems and other infrastructure against threats and adversaries, the community must invest in and prioritize the cybersecurity of OT and ICS networks using security controls that have demonstrated success against actual threats. Finally, the public and private sectors must work together using our unique capabilities and expertise to ensure that water and wastewater organizations have the tools and

resources they need to protect their systems. But all of this is predicated on addressing the economics and awareness of issues that exist at our local municipalities and town water systems.

I sincerely thank the subcommittee for providing me the opportunity to testify today and welcome any questions or requests for additional information.

Testimony of Dr. Charles Clancy

Chief Technology Officer, MITRE

before the House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection, Hearing on Securing Operational Technology: A Deep Dive into the Water Sector

6 February 2024

Chairman Garbarino, Ranking Member Swalwell, and Committee Members:

Thank you for inviting me to testify before you today on a topic of critical national importance. My name is Charles Clancy, and I am a Senior Vice President and Chief Technology Officer at MITRE where I lead science, technology, and engineering for the company. MITRE is a non-profit, non-partisan research institution that operates Federally Funded Research and Development Centers (FFRDCs) on behalf of the U.S. Government. Among other technical disciplines, our team of over 1,500 cybersecurity professionals provide deep expertise across the executive branch, including in support of organizations like the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and U.S. Cyber Command. MITRE's ATT&CK™ framework has become the *de facto* language between government and industry for describing and combatting cyber threats.

Prior to joining MITRE, I spent nine years as a member of the faculty at Virginia Tech where I held the Bradley Distinguished Professorship of Cybersecurity in the Department of Electrical and Computer Engineering, and served as executive director of what is now the Virginia Tech National Security Institute. I started my career at the National Security Agency leading advanced research and development programs.

It is my pleasure to address this committee.

Threat Environment

Threats to our nation's critical infrastructure cybersecurity have heightened dramatically over the past seven years as Russia and China have shifted to using cyber access to U.S. critical infrastructure as a strategic instrument of statecraft. Targeting and penetrating our infrastructure have grown precipitously, leading then Director of National Intelligence Dan Coats to famously say the "warning lights are blinking red again" in 2018[1], comparing warning signs about critical infrastructure penetrations to the pre-9/11 indicators. Just last week FBI Director Christopher Wray testified that the U.S. government had successfully disrupted Volt Typhoon[2], a persistent and sophisticated Chinese Communist Party (CCP) campaign to gain strategic access to U.S. critical infrastructure systems for disruptive and destructive effects.

In its 2023 annual threat assessment[3], the intelligence community assessed that the CCP would launch widespread cyber attacks against US critical infrastructure ahead of an invasion of Taiwan to "deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces." Their primary targets are assessed to be energy, transportation, communications, and water infrastructure.

With President Xi's asserted timeline of being ready for a Taiwan invasion by 2027[4], the U.S. military is kicking its response planning into high gear, but the U.S. may be existentially unprepared to defend its critical infrastructure for what would undoubtedly be an initial wave of attacks, followed by a sustained cyber campaign targeting U.S. infrastructure. Campaigns like Volt Typhoon demonstrate that this threat is not hypothetical: the CCP is deliberately gaining access to critical infrastructure so it can strategically disrupt and destroy these systems at a future time.

Much of the U.S. strategy to date has focused on strengthening our systems to keep adversaries out of our critical infrastructure and to blunt the first wave; however, this strategy fails to recognize that CCP attacks in conjunction with a Taiwan invasion will not be discrete events for which we can respond proportionately, but an enduring cyber conflict. Our current

---

[1] https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks
[2] https://www.washingtonpost.com/national-security/2024/01/31/china-volt-typhoon-hack-fbi/
[3] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
[4] https://www.reuters.com/world/china/logistics-war-how-washington-is-preparing-chinese-invasion-taiwan-2024-01-31/

approach is inadequate. Advanced persistent threat actors are frequently obviating protections we have placed in these systems. It also doesn't address the rapid response and restoration activities that will inevitably be needed to reconstitute when attacks occur.

Needed Strategic Posture

Much can be done to improve the current apparatus for securing critical infrastructure, and I will address those within the context of the water sector shortly. But I fear those actions miss the forest for the trees.

Nationally, we need to prepare for a more realistic adversary operational plan. Military systems have *wartime reserve modes* that change their configuration and operating posture to confound adversary exploitation, and the U.S.'s critical infrastructure systems need an intellectually similar set of contingencies that can be activated in a period of major conflict.

Many critical infrastructure operators already contemplate such impacts through the lens of natural disasters. For example, electric grid operators consider ways to minimize the impacts of geomagnetic disturbances from the sun by modifying the state and configuration of their operations. This operational adaptability mindset needs to extend to cyber-attack scenarios.

Operators need to prepare, train, and exercise for isolation operations where they operate their operational technology (OT) systems physically isolated from the information technology (IT) systems and the Internet. This includes creating continuity of operations plans that sever IT and OT systems to disrupt an adversary's ability to command and control malicious tools deployed into OT systems. Given CCP threat actors have adopted a strategy of "living off the land" where they do not install detectable malicious agents in target networks, but rather access systems like authorized administrators[5], severing IT-OT connectivity would prevent them from triggering effects to degrade or destroy critical infrastructure sytems.

Likely many critical infrastructure operators lack the needed engineering staff to sustain isolation operations in an ongoing capacity, so new programs are needed to train national guard units or create a civilian reserve corps of cyber physical operators and experts to augment critical infrastructure operators to sustain isolation operations. Moreover, we need to practice for multiple sector failures in population centers and assess cascading impacts. This includes not

[5] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

only tabletop exercises and hypothetical wargaming, but also live drills where we test contingency operations.

The cost of compliance is a common pushback to levying new responsibilities on private sector critical infrastructure asset-owner-operators, therefore, to incentivize adoption of cyber best practices, the federal government needs to reduce that burden. The Federal Emergency Management Agency (FEMA) should extend their existing grants program[6], in partnership with Sector Risk Management Agencies (SRMAs), to fund the necessary preparation, training, and exercises. The Cybersecurity Infrastructure Security Agency (CISA) should be resourced to manage a systematic exercise program to ensure that, if necessary, we have the national experience necessary to act under urgent circumstances.

Given the scale of the challenge, FEMA and CISA should focus on the current CISA *lifeline* sectors: energy, water, communications, and transportation[7].

Water Sector

The water sector is perhaps the most under resourced and disadvantaged among the lifeline sectors. In addition to preparing and practicing contingencies for a large-scale and enduring cyber conflict, there are plenty of more targeted things that could help improve cybersecurity and make China and Russia's cyber exploitation efforts more difficult.

Presidential Policy Directive (PPD) 21[8], *Critical Infrastructure Security and Resilience*, and PPD 41[9], *United States Cyber Incident Coordination,* organized the ecosystem we have today between CISA, the Federal Bureau of Investigation (FBI), and SRMAs. Accordingly, SRMAs bear the front-end regulatory responsibilities, while CISA and the FBI are responsible for back-end incident management and investigation after a cyber attack has occurred. There is a perception by operators, however, that systematically engaging SRMAs in incident response could lead to punitive regulatory actions. That, combined with their frequent lack of incident response experience and expertise, leads to an open loop system where we do not learn from

---

[6] https://www.cisa.gov/state-and-local-cybersecurity-grant-program
[7] https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
[8] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[9] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

attacks, which is antithetical to the goals of the NIST Cybersecurity Framework[10] and Executive Order 13636[11]. While sectors like the bulk electric power system[12] have been forced to ameliorate this through robust working-level relationships, public-private partnerships, and unique authorities held by the Secretary of Energy[13], other sectors such as water lack this scale, sophistication, and authorities.

At a national level, water's SRMA, the Environmental Protection Agency (EPA) needs to deepen its in-house cybersecurity expertise and develop a strategy to promote cybersecurity more effectively within the sector. This strategy should be informed by threat and incident information by EPA being much more engaged with CISA in incident response and analysis. The recently released incident response guide[14] is a good indicator that these connections are strengthening. Given the large number of water entities without any cybersecurity expertise and limited resources, implementation guidance, in plain language, will likely be needed to translate existing CISA, FBI, and NSA guidance to a simplified list of priority actions.

Grass-roots efforts being led by the Water Sector Coordinating Council and Water Information Sharing and Analysis Center (ISAC) are also important positive steps. In fact, both MITRE and Dragos are working closely with the Water ISAC on constructive solutions[15]. More broadly, MITRE has recommended SRMAs shift the focus from compliance checking to self-assessments, threat sharing, technical assistance, and fostering the organizational capacity and expertise execute[16].

Another important step is standardizing reporting of cyber incidents. Despite highlighting significant cybersecurity gaps within the water sector, prior EPA efforts were

---

[10] https://www.nist.gov/cyberframework
[11] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[12] https://www.nerc.com/pa/Stand/Pages/default.aspx
[13] https://www.energy.gov/ceser/energy-security-provision-within-fixing-americas-surface-transportation-act-fast-act
[14] https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide-0
[15] https://www.waterisac.org/portal/water-and-wastewater-utilities-and-other-critical-infrastructure-fortify-defenses-against
[16] https://www.mitre.org/sites/default/files/2023-11/PR-23-02057-08-Cybersecurity-Regulatory-Harmonization.pdf

withdrawn over legal challenges[17]. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022[18] offers the potential to close this gap if the information collected is robust and focused on reporting tangible threat behaviors and indicators. Similarly, improved coordination and interoperability among OT security vendors[19] could also help close the information and reporting gap.

Meanwhile, since Executive Order 14028[20], industrial capacity to generate and deliver software bills of material (SBOMs) has been improving. Open-source software underpins most of the Internet, and is also pervasive in OT networks. In most cases, this software has dubious supply chains[21] and critical infrastructure operators need tools to better manage this risk. One approach is to have OT vendors selling into the U.S. market provide SBOMs for their products to a clearinghouse that notifies them if a new vulnerability is disclosed that impacts their product. Much like safety recalls for automobiles governed by the National Highway Traffic Safety Administration (NHTSA), similar notices could be combined with regulatory rulemaking to prompt critical infrastructure operators to close security gaps in a timelier manner.

Conclusion

In closing, there is a considerable opportunity for EPA to step up, CISA and FBI to systematically engage across, and the network of security vendors to make it easier for everyone to coordinate. But these modest reforms should be kept in context with the scale of the threat, and the limited amount of resources available to critical infrastructure operators, particularly in the water sector. We should urgently begin piloting, exercising, and preparing for contingency scenarios that require isolated operations across lifeline critical infrastructure sectors.

---

[17] https://www.securityweek.com/epa-withdraws-water-sector-cybersecurity-rules-due-to-lawsuits/

[18] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[19] https://www.nozominetworks.com/blog/ethos-emerging-threat-open-sharing-platform

[20] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[21] https://industrialcyber.co/reports/fortress-research-finds-most-us-energy-software-contains-code-from-russian-chinese-developers/

American Water Works Association
Dedicated to the World's Most Important Resource®

Government Affairs Office
1300 Eye Street NW
Suite 701W
Washington, DC 20005-3314
T 202.628.8303
F 202.628.2846

U.S. House Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection
Hearing on Securing Operational Technology: A Deep Dive into the Water Sector

Testimony

Kevin M. Morley, PhD
Manager, Federal Relations
American Water Works Association

February 6, 2024

Good morning, Chairman Garbarino, Ranking Member Swalwell, and members of the Subcommittee. My name is Kevin Morley, and I am the Federal Relations Manager for the American Water Works Association (AWWA), on whose behalf I am speaking today. Established in 1881, AWWA is the largest nonprofit, scientific and educational association dedicated to managing and treating water, the world's most vital resource. We represent water systems large and small, municipal and investor-owned, urban and rural. With approximately 50,000 members, AWWA provides solutions to improve public health, protect the environment, strengthen the economy and enhance our quality of life. In the modern era of water utility operations, that mission also includes managing cybersecurity risks that could threaten the essential lifeline function water professionals provide 24/7/365.

IT & OT in the Water Sector

Drinking water and wastewater utility operations have been evolving and adapting to new technologies since the turn of the last century. A paper presented during AWWA's 1965 Annual Conference includes a statement that is just as relevant today as it was then:

> *The complex expansion of water systems has resulted in substantial adoption of instrumentation by the water industry. Modern instrument systems have made possible the surveillance and remote control of wells, treatment facilities, pumping stations, storage tanks, and transmission main valving, while rising labor costs have prompted water utility management to follow other industries in establishing some degree of automation and centralized control.*[1]

The difference today as it relates to cybersecurity is the convergence of technology systems that had traditionally operated independently. Information technology (IT) are the business enterprise systems like laptops and software systems used to manage email, payroll, customer billing, and service contracts. The operational technology (OT) are the systems used to manage and control various physical operations for the treatment and distribution of drinking water or the collection and treatment of wastewater. The integration of IT and OT systems has improved operational efficiency to optimize various unit processes and allowed greater visibility into those systems.

The challenge is that many current IT systems were designed to be connected to the internet, while OT systems were not but have since been plugged in. This integration began before the prospect of cybersecurity threats targeting today's critical infrastructure systems were envisioned. The cost savings realized were long ago absorbed into capital projects and

[1] Crow, W.B. & Eidsness, F.A (1965) Savings Through Instrumentation and Control In Two Water Systems. *Journal AWWA*, 57:12:1509.

reconfigurations of the workforce. Those OT systems were capital intensive and often had an expected service life of 20-25 years. This is very different than IT systems which have cycled through new versions at a pace that has outpaced the support for OT systems. As a result, older legacy OT systems are dependent on IT systems that are no longer supported and are unable to communicate with the new versions.

The "fix" for this digital divide is complex since utility services must continue working 24/7 until the transition is complete. While implementation of certain controls can help to manage cyber risk, ultimately IT upgrades may require total overhaul, rip and replace, of various OT elements. These capital projects are often lengthy and cost intensive. As an example, a large water system recently embarked on a 5-year, $80 million capital project to complete these upgrades. The financial cost associated with this type of transformation is amplified by the reality that 90% of water systems serve less than 3,300 people and have severely constrained budgets.

Drinking water utilities are already facing significant costs to comply with multiple regulations, including the revised lead and copper rule and pending PFAS standards. The treatment processes necessary to comply with these rules will require greater automation and digital dependency. The compliance costs for new regulatory obligations come on top of the $1.2 trillion that AWWA estimates is needed over 20 years for the repair and replacement of aging distribution and transmission lines nationally.[2] Escalating supply chain costs on essential treatment chemicals, piping materials and equipment have also imposed considerable pressure on operating budgets, which are not expected to moderate in the near term.[3]

Unlike other critical infrastructure sectors, to date, there has been no dedicated funding appropriated to expedite technology upgrades at water systems with legacy OT systems. While cybersecurity is one of many eligible activities within the State Revolving Fund (SRF) program,

[2] AWWA (2012) Buried No Longer: Confronting America's Water Infrastructure Challenge.
[3] Morley, KM. (2023) Supply Chain Threats Persist. *Journal AWWA* 115(2):6. https://doi.org/10.1002/awwa.2048

constraints on that program may not allow utilities to acquire the optimal cybersecurity support they need. If the water sector is truly a national security priority, then it will need support to expedite technology transformations to address the digital divide in a manner that is not punitive and fulfills our shared commitment to the communities we serve.

Prioritizing Cybersecurity in the Water Sector

Drinking water and wastewater systems sustain our way of life and support public health, safety and economic vitality. These systems are robust and resilient but, like all critical infrastructure entities, are not immune to cyber threats. In recognition of this threat, AWWA has actively engaged our members, and the sector at large, in building cybersecurity awareness and providing resources to support the implementation of best practices. As evidence of growth in awareness, utility leaders have consistently rated cybersecurity as a very high priority in AWWA's annual State of the Water Industry report for several years. This trend runs parallel to AWWA's collaboration with water utility subject matter experts and federal partners to provide a water sector-specific approach for implementing the NIST Cybersecurity Framework (CSF), as called for in Executive Order 13636.

AWWA's Water Sector Cybersecurity Risk Management Guidance and Assessment Tool, first issued in 2014, helps a utility examine which cybersecurity controls and practices are most applicable based on the technology applications they have implemented. The resource emphasizes actions that address the highest priority controls expected to quickly provide the greatest risk reduction value. AWWA also partnered with the United States Department of Agriculture to develop the Water Sector Cybersecurity Risk Management Guidance for Small Systems, a "getting started guide" that helps small, rural utilities serving fewer than 10,000 people assess and implement cybersecurity best practices.

Strong cybersecurity measures are essential to ensuring a cyber incident does not threaten public health. Several cyber incidents led AWWA in 2021 to assess a variety of

potential options, which resulted in our recommendation to establish a new cybersecurity governance framework in the water sector. Our recommended approach would create an independent, non-federal entity to lead the development of minimum cybersecurity requirements, leveraging subject matter experts from the water sector. Federal oversight and approval of requirements would be provided by the EPA. This framework builds on a similar model that has been applied in the electric sector with congressional approval.

This governance model would follow a tiered, risk- and performance-based approach that accommodates the differences in operational complexity and maturity in the sector. This recommendation aligns with calls for public-private collaboration included in the National Cyber Strategy. It recognizes that cybersecurity is a shared responsibility that benefits from the direct engagement and operational knowledge of owner/operators and the accountability that comes with federal oversight.

We believe it is timely and prudent for Congress to authorize this collaborative model to ensure utilities are directly engaged in developing appropriate cybersecurity requirements -- with oversight from EPA – to create a robust cybersecurity risk management paradigm in the water sector.

In addition to establishing a sound oversight model, it is critical to recognize other collaborative opportunities to support cybersecurity in the water sector.

Consistent Public-Private Collaboration

CISA's maturity has evolved significantly since its formation, including predecessor functions. Most notable is the permanent addition of a water sector liaison in the Stakeholder Engagement Division. This has provided continuity in communications and generated productive engagement with the Water Sector Coordinating Council (SCC) and EPA as the Sector Risk Management Agency (SRMA). The most recent output was a stakeholder engagement process facilitated by the Joint Cyber Defense Collaborative (JCDC) which

published "Incident Response Guide: Water and Wastewater Systems (WWS) Sector." This effort integrated the insights and recommendations provided by the stakeholder community to ensure that the guidance is best suited address their needs.

Another useful outcome was a collaborative effort to raise the visibility and awareness of CISA's Vulnerability Scanning service, as recommended in prior testimony. Before the fact sheet developed with the WSCC and Association of State Drinking Water Administrators, the value and purpose of this tool was not accessible to the entities that would derive the greatest benefit if enrolled. The fact sheet requires an organized outreach campaign that can provide a unified message on the resources provided by CISA and their relationship with other resources.

In the earlier years of CISA's predecessor, the SCCs would come together with agency staff for strategic planning, a requirements assessment of sorts, to identify the needs of the various critical infrastructure sectors. While not all sector needs became action items for agency workplans, it was a useful exercise to examine unique conditions and identify cross-sector needs. The WSCC, working with state and federal partners, has developed a strategic roadmap that defines top-level priorities for managing risk and building resilience. When federal partners initiate projects to act on those priorities, it is in our collective interest that collaboration occurs early and often to ensure the approach is aligned with the needs of the stakeholders for whom it is presumably designed to support. Miscues lead to missed opportunities, duplication of effort and products that do not fulfill the needs of owner/operators.

As we did following 9/11, collaboration with trusted partners like AWWA is a high value force multiplying capability that should be maximized to address the national security risk cyber threats impose on drinking water and wastewater systems. Other action items to be considered further include the following:

1. **Unified Messaging**. Launch a collaborative campaign to expedite enrollment in CISA's vulnerability scanning service to help utilities address threat exposure. This is a highly valuable service for systems with limited in-house resources to provide timely information on exposures and recommended mitigations.

Work with stakeholders in the water sector to review the myriad resources and prepare a matrix that communicates, in plain English, the function they provide and associated relationship. Currently, the array of "stuff" is overwhelming and as a result undersubscribed or inaccessible to those with the greatest need, absent some order or clearly defined progression of applicability.

2. **Inform and Enable.** Invest in capacity development to empower utility owner/operators to effectively engage cybersecurity issues that are aligned with their needs. We believe AWWA's small system guidance provides a robust "getting started" guide focused on six key domains from the NIST CSF.

   Training on the application of this guidance delivered by trusted partners like AWWA is a highly effective and proven force multiplier for building awareness and enabling utilities to assess potential vulnerabilities and implement control to mitigate risks. There is a significant opportunity to collaborate to support the cybersecurity needs for 50,000 community drinking water systems and nearly 16,000 wastewater systems.

3. **Technology Transformation**. Funding that prioritizes and expedites technology upgrades to address legacy operational technologies will be necessary to overcome the growing digital divide. These legacy OT systems simply cannot operate on newer enterprise platforms and, in many instances, this requires a rip and replace project that is capital and time intensive.

4. **Improve threat information sharing**. We recommend that CISA and EPA work with partners like the WaterISAC and the Water Sector Coordinating Council to establish a standard operating procedure for the inclusion of SMEs in the development of threat alerts and advisories to ensure that the information transmitted is concise, actionable, and properly contextualized.

   In addition, it is critical to recognize and address the unconscious competence associated with many cybersecurity advisories. Simply state the problem and the recommended mitigation. We would recommend putting the TTPs and MITRE Attack explanation in an appendix, as they are interesting but often a distraction from the action being recommended to mitigate the threat.

5. **Research and Development.** The Water Security Test Bed (WSTB), developed by Idaho National Laboratory (INL) and the EPA Office of Research and Development's (ORD), can help support research into water sector-specific vulnerabilities and coordinate information sharing. The WSTB is a large-scale, adaptable testing environment that can be disrupted or destructively tested by government and industry partners. Funding for this program would provide an objective platform to evaluate cyber intrusion scenarios, demonstrate physical impacts, deliver scalable mitigations useful for water utilities of various sizes and budgets, and provide realistic utility operator training.

##################

Kevin M. Morley, PhD

Kevin M. Morley, PhD is Manager, Federal Relations for the American Water Works Association (AWWA). Over the past 20 years he has worked closely with multiple organizations to advance security and preparedness in the water sector. This includes establishing the Water/Wastewater Agency Response Network (WARN) and guiding the development of several ANSI/AWWA standards that represent minimum best practices for water sector risk and resilience management, including cybersecurity. He is a leading expert on §2013 of America's Water Infrastructure Act (AWIA) of 2018 and multiple resources that enable water systems to implement an all-hazards approach to security and preparedness. Dr. Morley has supported the national discourse on risk and resilience as a Disaster Resilience Fellow for the National Institute of Standards and Technology, a member of the President's National Infrastructure Advisory Council and the Water Sector Coordinating Council. Dr. Morley received a PhD from George Mason University for research developing the Utility Resilience Index (URI). He holds a MS from the State University of New York College of Environmental Science and Forestry and a BA from Syracuse University.

################

What is the American Water Works Association?

The American Water Works Association (AWWA) is an international, nonprofit, scientific and educational society dedicated to providing total water solutions to protect public health and assure the effective management of water. Founded in 1881, the association is the largest organization of water professionals in the world.

Our membership includes more than 4,500 utilities that supply roughly 80 percent of the nation's drinking water and treat almost half of the nation’s wastewater. Our 50,000 members represent the full spectrum of the water community: public water and wastewater systems, environmental advocates, scientists, academicians, and others who hold a genuine interest in water, our most important resource.

AWWA is accredited by ANSI (American National Standards Institute) as a standards development organization and publishes over 170 Standards that provide valuable information on design, installation, disinfection, performance, and manufacturing of products including pipe, chemicals, storage tanks, valves, meters and other appurtenances; industry-recognized consensus prerequisites; and best practices for water utility management and operations. AWWA unites the diverse water community to advance public health, safety, the economy, and the environment.

###

################

What is the American Water Works Association?

The American Water Works Association (AWWA) is an international, nonprofit, scientific and educational society dedicated to providing total water solutions to protect public health and assure the effective management of water. Founded in 1881, the association is the largest organization of water professionals in the world.

Our membership includes more than 4,500 utilities that supply roughly 80 percent of the nation's drinking water and treat almost half of the nation’s wastewater. Our 50,000 members represent the full spectrum of the water community: public water and wastewater systems, environmental advocates, scientists, academicians, and others who hold a genuine interest in water, our most important resource.

AWWA is accredited by ANSI (American National Standards Institute) as a standards development organization and publishes over 170 Standards that provide valuable information on design, installation, disinfection, performance, and manufacturing of products including pipe, chemicals, storage tanks, valves, meters and other appurtenances; industry-recognized consensus prerequisites; and best practices for water utility management and operations. AWWA unites the diverse water community to advance public health, safety, the economy, and the environment.

###

Marty Edwards
Deputy CTO OT/IoT, Tenable, Inc.
House Homeland Security Committee
Subcommittee on Cybersecurity and Infrastructure Protection
"Securing Operational Technology: A Deep Dive into the Water Sector "
February 6, 2024

Introduction

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and members of the Subcommittee, thank you for the opportunity to testify before you today on securing the industrial control systems that underpin our nation's water sector.

My name is Marty Edwards and I am the Deputy Chief Technology Officer for Operational Technology (OT) and Internet of Things (IoT) at Tenable, a cybersecurity exposure management company that provides organizations, including the federal government, with an unmatched breadth of visibility and depth of analytics to measure and communicate cybersecurity risk. In collaboration with industry, government, and academia, Tenable is raising awareness of the growing security risks impacting critical infrastructure and the need to take steps to mitigate those risks.

My expertise is in OT and Industrial Control System (ICS) cybersecurity, and my work with Tenable has focused on furthering government and industry initiatives to improve critical infrastructure security. I also previously served as the working group lead in the development of the Information Technology (IT)/OT Convergence Report[1] issued by The President's National Security Telecommunications Advisory Committee (NSTAC) in August 2022.

Prior to joining Tenable, I worked in the industry as an Industrial Control Systems Engineer and as a Program Manager at the U.S. Department of Energy's Idaho National Laboratory focused on cybersecurity. I was the last and the longest-serving Director of the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which is now part of the Cybersecurity and Infrastructure Security Agency (CISA).

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure nearly any digital asset on any computing platform, including OT and IoT. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.[2]

---

[1] President's National Security Telecommunications Advisory Committee, "Information Technology and Operational Technology Convergence Report," https://www.cisa.gov/sites/default/files/publications/NSTAC%20IT-OT%20Convergence%20Report_508%20Compliant_0.pdf

[2] Tenable, "About Tenable," www.tenable.com

Why OT and Why Now

On January 31, 2024, news broke that the U.S. disrupted attempts by China to plant malware within U.S. critical infrastructure systems, including water treatment plants. That same day, General Paul Nakasone, Commander of U.S. Cyber Command; Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA); Christopher Wray, Director of the Federal Bureau of Investigation (FBI); and Harry Coker, Jr., Director of the Office of the National Cyber Director (NCD), appeared before your colleagues on the House Select Committee on the Chinese Communist Party (CCP).

The testimonies of these four cyber leaders addressed the threats to our critical infrastructure. Director Wray stated that, "cyber threats to our critical infrastructure represent real world threats to our physical safety,"[3] and Director Easterly echoed that sentiment, saying **"cybersecurity is national security."**[4]

Tenable CEO Amit Yoran responded to Director Wray's comments, calling his warning "an urgent call to action. Continuing to turn a blind eye to the risk sitting inside our critical infrastructure is the definition of negligence."[5]

Efforts to infiltrate the underlying systems that support not only the daily lives of Americans but also our economy are emerging as an acute national security risk. Cyber attacks against water systems can cause significant health effects, render property uninhabitable, and displace entire communities. We live in a digital world, and as a nation we must accept that our national security defense requires securing the IT and OT systems that keep U.S. critical infrastructure operational.

While government and industry OT security initiatives are moving in the right direction, another key component to ensuring success is federal funding. As Tenable CEO Amit Yoran stated in a recent letter to congressional appropriators, robust cybersecurity funding must continue to be prioritized to ensure we can meet the cyber threats of today while securing against those of tomorrow.[6]

There is no doubt that the history of OT systems and the current challenge of IT/OT/IoT convergence makes securing our critical infrastructure all the more difficult. However, we have the tools, knowledge, and capabilities to be successful.

The Complicated History of Securing Operational Technology

While OT has always been part of utilities, manufacturing, and other critical infrastructure sectors, OT technology was considered "safe" from attacks because most OT devices were not connected to outside networks. It has been commonplace for software-dependent systems to be placed into service and never touched again for the next ten years, resulting in OT systems left unincorporated into standard processes for regular software updates, vulnerability assessments and risk mitigation practices. With the

[3] House Select Committee on the Chinese Communist Party, "The CCP Cyber Threat to the American Homeland and National Security," testimony of FBI Director Christopher Wray (22:10), https://www.youtube.com/watch?v=MJOX3cpHfUI

[4] House Select Committee on the Chinese Communist Party, "The CCP Cyber Threat to the American Homeland and National Security," testimony of CISA Director Jen Easterly (36:10), https://www.youtube.com/watch?v=MJOX3cpHfUI

[5] https://apnews.com/article/fbi-china-espionage-hacking-db23dd96cfd825e4988852a34a99d4ea

[6] Amit Yoran, "Support for Prioritizing CISA Funding," LinkedIn, November 8, 2023, https://www.linkedin.com/posts/ayoran_support-for-cisa-activity-7128398109985935360-xj7C/

convergence of IT and OT in today's modern facilities, these devices are often no longer air-gapped and in many cases are exposed to the internet — and to the threat of ransomware and cyberattacks.[7]

The siloed nature of cybersecurity, especially between IT and OT teams, presents additional challenges for those tasked with securing OT. OT systems have yet to advance their security posture to be on par with their IT counterparts. In addition, IT and OT systems have their own goals and priorities, performance requirements, purposes, and lifecycles. To reduce cyber risk, organizations worldwide must consider the deeply entrenched people, process, and technology issues within both IT and OT.[8]

OT and IoT systems require specialized asset discovery solutions in order to not disrupt the safety and reliability of these environments. However, in a converged system-of-systems, asset owners must continuously evaluate all aspects of their systems, to include IT, OT, IoT, Cloud, Asset Exposure, and Identity. If all of these characteristics are being measured by separate security systems, it can make the CISO's job to provide concise, consolidated reporting difficult. Modern exposure management platforms can provide this overarching measurement of risk that can then be communicated to senior executives or to boards of directors.

Today's environment brings numerous opportunities for misconfigurations and overlooked assets which makes it nearly impossible for cybersecurity leaders to obtain a unified view of their exposure. Too often, cybersecurity professionals develop an orientation toward reactive, incident-focused practices. Therefore, preventive tasks are often relegated to nothing more than a compliance exercise which leaves security teams unable to effectively evaluate what's happening across the attack surface.

It has long been challenging for organizations to reduce cyber exposure with existing preventive tools. The new expanding complexity of the modern attack surface – encompassing multiple cloud systems, numerous identity and privilege management tools, multiple web-facing assets along with OT and IoT systems and software – can make exposure management all the more difficult.

Security professionals need a unified view of their environments to realistically identify the objective security truths that indicate their exposure to risk. For operators of critical infrastructure environments, practices focused on cybersecurity governance, risk, and compliance must be revamped to improve exposure visibility. Management and remediation of security weaknesses in OT systems must be as routine a part of plant maintenance as the mechanical servicing of hardware.

The State of Operational Technology in the Water Sector

Recent Threats

In recent years, there has been an increase of successful cyberattacks against U.S. water systems and utilities, as well as wastewater systems. California, Maine, and Nevada's water facilities have all fallen victim to ransomware attacks. These attacks are continued evidence that industrial security is in need of

[7] Tenable, "Operational Technology (OT) Security: How To Reduce Cyber Risk When IT and OT Converge," https://www.tenable.com/source/operational-technology

[8] Tenable, "Zero Day Vulnerabilities in Industrial Control Systems Highlight the Challenges of Securing Critical Infrastructure," https://www.tenable.com/blog/zero-day-vulnerabilities-in-industrial-control-systems-highlight-the-challenges-of-securing

significant improvements. In addition, some level of government regulation is necessary to ensure the cyber safety of water and wastewater systems.

More recently, the Municipal Water Authority of Aliquippa, Pennsylvania was the target of the exploitation of Unitronics' programmable logic controllers (PLCs).[9] Programmable logic controllers (PLCs) are common tools utilized in the water and wastewater sectors. The exploitation of PLCs and similar OT systems are not new nor uncommon, but this set of attacks took advantage of direct internet accessibility, which enables control systems assets to be accessed remotely.

In a water or wastewater facility, PLCs are the literal brains of the operation. They are often programmed to do virtually all of the operational functions at a water treatment plant. When PLCs are compromised, threat actors can take control of motor and pump functions, and manipulate chemical settings. The effects on water quality and safety can be immediate or programmed to cause disruption at a future time.

Attacks such as the one in Aliquippa, Pennsylvania, are largely due to poor cyber hygiene. Bad actors can easily roam the internet in search of assets that still have the factory default password. Allowing for direct accessibility from the internet, default passwords, and a lack of authentication security is more than negligent; it is a failure of not only the asset owner but of the complete OT security environment. The attack on Aliquippa's Municipal Water Authority underscores the critical need to enhance security measures within the water sector. This, along with robust multi-factor authentication, is imperative for critical infrastructure organizations to strengthen their cybersecurity posture.

Federal Support for Bolstering Sector Security

In an effort to safeguard U.S. water and wastewater systems, CISA partnered with the Environmental Protection Agency (EPA) to develop a comprehensive toolkit designed to "help water and wastewater systems build their cybersecurity foundation and progress to implement more advanced, complex tools to strengthen their defenses and stay ahead of current threats."[10]

Additionally, CISA, the FBI and the EPA recently issued a joint water sector incident response guide, which was developed under the Joint Cyber Defense Collaborative (JCDC), with participation from Tenable. The guide provides an extensive range of resources that cover the four stages of the incident response lifecycle, from preparation to proactive post-incident activities. The guide also offers best practices for cyber incident reporting. CISA Executive Assistant Director for Cybersecurity Eric Goldstein emphasized, "In the new year, CISA will continue to focus on taking every action possible to support 'target-rich, cyber-poor' entities like WWS utilities by providing actionable resources and encouraging all organizations to report cyber incidents."[11]

---

[9] CNN, "Federal investigators confirm multiple US water utilities hit by hackers," https://www.cnn.com/2023/12/01/politics/us-water-utilities-hack/index.html

[10] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Water and Wastewater Cybersecurity Toolkit," https://www.cisa.gov/water

[11] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "CISA, FBI and EPA Release Incident Response Guide for Water and Wastewater Systems Sector," https://www.cisa.gov/news-events/news/cisa-fbi-and-epa-release-incident-response-guide-water-and-wastewater-systems-sector

The EPA also issued – and then rescinded – its cybersecurity rule which mandated that states evaluate the cybersecurity capabilities of their drinking water systems. This mandate included assessing the cybersecurity of their public water systems' OT environment. Despite the rule no longer being in effect, the EPA continues to recommend aligning cybersecurity practices with CISA's CPGs.[12] Tenable strongly encourages water infrastructure entities to follow this guidance as it empowers users to inventory assets, proactively assess vulnerabilities, implement robust cybersecurity protocols, and mitigate potential risks to build resilient water and wastewater systems.

It is worth noting that following the EPA's decision to rescind its cyber rule, there have been significant efforts within the water sector to support a collaborative approach with federal partners to develop a framework similar to that employed by the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) in the electric sector.[13] We are pleased to see this high level of stakeholder engagement in the development phase and the strategic utilization of preexisting successful frameworks to enhance cybersecurity in the water sector. However, while this long-term initiative is considered, it is imperative that we also support more immediate actions. CISA's CPGs should be the blueprint for implementing effective risk reduction practices in the interim.

There is no denying that foreign adversaries will continue to target the U.S. water sector and its more than 148,000 public water systems. How we address vulnerabilities today and build security into future systems will be the most important factors in determining the outcome of a large-scale targeted attack on our water infrastructure. Government officials and private sector leaders must stay focused on addressing critical infrastructure vulnerabilities, particularly those stemming from the convergence of IT and OT technologies.[14] Tenable firmly believes this is a national security imperative.

Current Federal Initiatives Improving OT and IoT Security

Until recently, federal resources have primarily focused on securing IT networks. While this focus was more understandable prior to the convergence of IT and OT, the modern attack surface is rapidly expanding. Cyber criminals continue to use effective tactics such as exploiting known but unpatched vulnerabilities and deploying ransomware to gain entry into and compromise unsecured OT systems.

There are several federal initiatives to help OT organizations address modern security challenges, including Pillar One of the Administration's National Cybersecurity Strategy, CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), the CISA Cyber Hygiene program, the JCDC Industrial Control Systems (ICS) Working Group, the CyberSentry program, and the EPA's Cybersecurity Resources for Drinking Water and Wastewater Systems. Additionally, efforts like The President's National Security Telecommunications Advisory Committee (NSTAC) resulted in recommendations to improve IT/OT convergence. CISA's BOD 23-01 is helping federal civilian departments and agencies identify assets and prioritize OT vulnerabilities. Finally, partnerships like the OT Cybersecurity Coalition (OTCC) are bringing

[12] Regulatory Oversight, "EPA Withdraws Cybersecurity Rule for Public Water Systems," https://www.regulatoryoversight.com/2023/11/epa-withdraws-cybersecurity-rule-for-public-water-systems/

[13] American Water Works Association, "AWWA repeats call for strong cybersecurity measures after EPA withdraws rule,"https://www.awwa.org/AWWA-Articles/awwa-repeats-call-for-strong-cybersecurity-measures-after-epa-withdraws-rule

[14] U.S. Environmental Protection Agency, "Information about Public Water Systems," https://www.epa.gov/dwreginfo/information-about-public-water-systems

together industry and government stakeholders to better protect ICS and critical infrastructure assets. The following initiatives discussed below provide direction and guidance to improve OT cybersecurity outcomes.

Pillar One of the Administration's National Cybersecurity Strategy prioritizes establishing best practices and expanding minimum cybersecurity standards, including basic cyber hygiene and secure-by-design principles. The Strategy highlights the persistent security threat of IT/OT convergence, prompting organizations to strategize responses to these challenges.[15]

CISA's CPGs are a voluntary baseline of cybersecurity practices for all critical infrastructure entities that align with functions of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), which is widely utilized by critical infrastructure owners and operators. These goals integrate recommended practices for both IT and OT owners to prioritize security measures. Primary among these recommended practices is the requirement of a role to oversee all OT-related cybersecurity activities which will strengthen the relationship between IT and OT teams, improve incident response times, and provide OT-specific training for individuals in charge of OT operations. While a crucial step forward, it is necessary to acknowledge that additional efforts are needed, particularly to fortify the security of OT systems, especially those on which our nation's water sector depends.

CISA's Cyber Hygiene Program provides critical infrastructure facilities with essential services, including network discovery and vulnerability reporting. However, the number of eligible entities that participate in this valuable service is limited. There is an opportunity for CISA to enhance the promotion of these services and expand them to cover assessments of OT systems and networks. Further, Congress should ensure the program is adequately funded so that a greater number of resource-poor crucial infrastructure entities and utilities can improve their baseline cyber defenses.

CISA recently established an ICS working group within the JCDC , which enables collaboration with CISA across a range of cybersecurity and vulnerability management issues, including bolstering the cybersecurity and resiliency of OT systems. Managing vulnerabilities is essential to secure critical IT and OT infrastructure and the work done by JCDC and CISA promotes the prioritization of network security. *Tenable is a proud Alliance Partner of the JCDC.*

The CyberSentry Program was also established by CISA as part of its ongoing commitment to safeguarding the nation's critical infrastructure against sophisticated cyber threats. This threat detection and monitoring capability, managed by CISA, collaborates closely with critical infrastructure providers to vigilantly monitor and detect cyber threats targeting both IT and OT networks. CyberSentry facilitates collective defense and mutual benefit across the critical infrastructure landscape through these partnerships. It provides IT and OT network operators with comprehensive visibility into both known and unknown assets, which is essential for effectively assessing and managing risks.

[15] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The EPA provides cybersecurity guidance and resources for drinking water and wastewater systems.[16] The "EPA Cybersecurity for the Water Sector" guide includes resources for cybersecurity assessments, planning, training, and response, as well as funding options available for water utilities.[17]

NSTAC's 2022 IT/OT Convergence Report recommendations have been impactful for improving OT security.[18] The report included three recommendations that the Administration could immediately implement to strengthen the cybersecurity posture of U.S. government owned and operated OT systems. To date, only one of those three recommendations has been partially implemented.[19]

The report recommended that the President issue a **Binding Operational Directive (BOD)** (similar to what Section 1505 of the Fiscal Year 2022 National Defense Authorization Act (NDAA) requires for the Department of Defense (DoD)) to require executive civilian branch departments and agencies to maintain a real-time, continuous inventory of all OT devices, software, systems, and assets within their areas of responsibility. The BOD should also require such inventory to include an understanding of any interconnectivity to other systems. Following the release of the NSTAC report, CISA issued BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks.[20]

Binding Operational Directive 23-01 was issued in October of 2022, and requires federal agencies to enhance visibility into agency assets and associated vulnerabilities. The BOD will help federal agencies have the necessary foundation to maintain a successful cybersecurity program, focusing on two core activities: Asset Discovery, and Vulnerability Enumeration.

This directive applies to all IP-addressable networked assets that can be reached over IPv4 and IPv6 protocols and outlines new requirements for cloud assets, IPV6 address space, and OT in an effort to reduce cyber risk. It builds on BOD 22-01, which was issued in 2021, and requires federal agencies "to remediate vulnerabilities in the Known Exploited Vulnerabilities (KEV) catalog within prescribed timeframes."[21] The KEV catalog is maintained by CISA and helps organizations prioritize remediation of listed vulnerabilities and reduce the opportunities for threat actors to compromise systems.

Additionally, in December of 2023 the **Office of Management and Budget (OMB) issued a memorandum (memo M-24-04)** to federal departments and agencies requiring IoT and OT asset inventory, in an effort to "enhance the U.S. Government's overall cybersecurity posture and to help

[16] U.S. Environmental Protection Agency Cybersecurity for the Water Sector, https://www.epa.gov/waterresilience/cybersecurity-assessments
[17] Ibid.
[18] Ibid 1.
[19] Tenable, "IT/OT Convergence: Now Is The Time to Act," https://www.tenable.com/blog/itot-convergence-now-is-the-time-to-act
[20] https://www.cisa.gov/news-events/directives/bod-23-01-improving-asset-visibility-and-vulnerability-detection-federal-networks
[21] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Reducing the Significant Risk of Known Exploited Vulnerabilities," https://www.cisa.gov/known-exploited-vulnerabilities

ensure integrity of systems."[22] The OMB set a deadline for agencies to inventory assets by the end of Fiscal Year 2024.

While the release of BOD 23-01 and M-24-04 are positive directions for federal agencies, there remain challenges with implementation. Compared to the IT environment, where patching, upgrading and replacing systems is standard, an OT environment typically requires working with legacy technologies. To prioritize remediation efforts, agencies need a detailed view of OT and IT assets in the OT environment and the ability to map connections between devices and identify high-risk assets.

To ensure that Federal Civilian Executive Branch (FCEB) systems, and agencies operating those systems, meet said requirements, Congress should appropriate funding to implement CISA's BOD 23-01, and OMB M-24-04. This will enable agencies to maintain an updated inventory of assets, identify software vulnerabilities, track how often an agency enumerates its assets, and share information with CISA's Continuous Diagnostics and Mitigation Program (CDM) Federal Dashboard. Pursuant to BOD 23-01, the scope of this implementation encompasses all reportable OT and IT assets.

The OTCC brings together a range of OT cybersecurity and technology providers to promote the use of standards-based, interoperable cybersecurity solutions to help critical infrastructure and other organizations defend themselves against growing threats. The OTCC also works with government stakeholders to promote effective operational technology cybersecurity.

Policy Recommendations

Tenable recommends that Congress enact the following policy objectives to enhance the cyber preparedness of U.S. critical infrastructure:

- **Establish baseline cybersecurity requirements or standards of care for critical infrastructure that align with CISA's Cross-Sector Cybersecurity Performance Goals, international standards, and the NIST CSF, based on effective cyber hygiene and preventive security practices.** Basic cyber hygiene for critical infrastructure operators includes continuous understanding of what assets are on networks, ensuring strong identity and access management, discovering and patching known vulnerabilities, and implementing incident detection and response capabilities. For critical infrastructure providers, these baseline requirements must address the challenges of securing converged IT and OT environments. Pillar One of the recently released National Cybersecurity Strategy calls for baseline cybersecurity requirements for critical infrastructure providers. The CISA Cross-Sector Cybersecurity Performance Goals, based on the NIST CSF, are an excellent resource for industry and Sector Risk Management Agencies to utilize in the development of baseline requirements and standards of care.

- **Prioritize robust cybersecurity funding** for programs and initiatives that support improving OT security, including:

[22] Office of Management and Budget, "Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements," https://www.whitehouse.gov/wp-content/uploads/2023/12/M-24-04-FY24-FISMA-Guidance.pdf

- CISA Cyber Hygiene services, to provide expanded services, including OT and IoT assessments, to critical infrastructure entities and utilities, enabling them to achieve a minimum cybersecurity posture.
- CISA and FCEB agencies, to implement BOD 22-01, and BOD 23-01, and M-24-04 policy recommendations. Protecting our nation's cybersecurity means knowing what is on our networks and maintaining such networks in good working order, which includes conducting an inventory of OT assets and prioritizing remediation of known vulnerabilities. If an organization does not know an asset exists, it cannot assess it for vulnerabilities. With the issuance of BOD 23-01, federal agencies need comprehensive visibility into their assets and vulnerabilities across their organization. This includes:
  - External unknowns
  - Cloud workload and resources
  - Operational technology
  - Network infrastructure and endpoints
  - Web application
  - Identity systems
- CISA and the Office of the National Cyber Director, to ensure they can meet mission requirements. The threats to federal networks and critical infrastructure are growing at a significant rate and CISA must serve as an effective coordinator to strengthen security in these environments. *Tenable supported the creation of the Office of the National Cyber Director and applauded efforts to stand up this office.*

- **Ensure that cybersecurity is incorporated for infrastructure grant funding.** Modern infrastructure projects increasingly leverage digital technologies and network connectivity. OT cybersecurity should be addressed in all federal infrastructure grant projects and should be an allowable expense for infrastructure grant recipients.

- **In its oversight of CISA implementation of CIRCIA, Congress should ensure that CISA is adequately resourced** to ingest the wealth of information that will be shared by critical infrastructure entities. CISA should request and share anonymized cyber incident data. It should provide actionable information through trusted partners, such as JCDC Alliance Partners, to provide cyber situational awareness to the broader critical infrastructure ecosystem. Finally, CISA should move towards automated and machine readable formats to ingest and share this information to the full extent possible.

- **Continue implementation of the NSTAC IT/OT Convergence Report policy recommendations**.
  - **Direct federal civilian agencies to inventory their OT assets and provide OT asset and vulnerability information to the CDM Dashboard.** CISA has already taken steps to address this obstacle through BOD 23-01, but Congress should reinforce the need to gain visibility into these mission-critical environments so we can understand the scale of cybersecurity challenges and begin to systematically address serious risks. The foundation for every security framework, whether IT or OT, always begins with visibility into the assets for which you are responsible. Achieving this visibility is a significant step forward for federal departments and agencies to protect their critical IT and OT assets against evolving cybersecurity threats.

- **Develop enhanced OT-specific cybersecurity procurement language.** Public and private sector OT procurements should require the inclusion of risk-informed cybersecurity capabilities for products and services. Updating procurement language guidance will help asset owners specify that cybersecurity be built into products and projects rather than bolted on as an afterthought. Including cybersecurity in both government and private sector procurement vehicles will significantly enhance the resilience of critical infrastructure systems.
- **Implement standardized, technology-neutral, real-time interoperable information sharing mechanisms** to promote the sharing of sensitive information across agencies and to break the traditional siloed approach. Cyberattacks often target multiple critical infrastructure sectors and attackers have the ability to move at machine speed to compromise multiple industrial sectors. Our defenses need to match this threat. It is imperative for our critical infrastructure sectors to securely communicate with each other to get the right information to the right person, at the right time. This requires a standardized, technology-neutral approach, in order to leverage cyberthreat and vulnerability information from the broader critical infrastructure ecosystem.

- **Support the JCDC and provide oversight of CISA to clarify roles and responsibilities of other public-private partnerships.** Congress should continue to support the JCDC as it advances strategic planning and incident response capabilities for the industry. However, it is important for Congress to provide robust oversight of CISA's JCDC efforts to ensure there is a clear delineation of roles and responsibilities and appropriate opportunities for industry to engage. Congress should also provide oversight to ensure that JCDC adequately addresses OT cybersecurity risks, threats and operational response capabilities.

- **Improve the ICS cyber workforce** by ensuring CISA implements the ICS cybersecurity training initiative included in Ranking Member Swalwell's Industrial Control Systems Cybersecurity Training Act, which was passed as part of the FY 2024 Defense Authorization bill.

- **Require Independent Assessments of critical software (to include OT and IoT).** CISA should apply the Sarbanes-Oxley "separation of duties" principles to cybersecurity and prohibit the provider responsible for developing and/or running critical software from also conducting its exposure management or otherwise testing its security, conducting security audits, or reporting on its security.

Conclusion

There are fundamental steps all federal agencies and critical infrastructure entities must take to improve their OT cybersecurity posture. Security professionals need visibility into which assets are on their networks and whether those assets are vulnerable. Known exposures should be addressed in a timely manner and user access and privileges must be effectively controlled. Finally, security teams must have unified visibility into, and management of, interconnected critical systems. These steps make it more difficult for bad actors to compromise interconnected IT and OT systems. Government policy can help drive these effective practices for critical infrastructure owners and operators.

Risk assessment and asset inventory processes are desperately needed as rapid expansion of access and interconnectivity dramatically increase risk**.** Policy guidance for minimum security requirements and standards of care are needed to help drive improvements in risk management practices while at the same time act to foster innovation. Government support and funding are necessary to strengthen cybersecurity programs for critical infrastructure providers which lack the resources to protect themselves from malicious actors. Finally, stakeholder engagement through public-private partnerships and other collective defense efforts can improve cyber situational awareness, strengthen policy guidance, and enhance broad adoption of cybersecurity best practices.

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and members of the Subcommittee, thank you for the opportunity to testify before you today on the critical matter of securing the industrial control systems vital to our nation's water sector. I appreciate the work this committee is doing to elevate cybersecurity issues with bipartisan support. I look forward to ongoing collaboration to safeguard the IT/OT/IoT systems that form the foundation of our nation's critical infrastructure.