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.