Marty Edwards
Deputy CTO OT/IoT, Tenable, Inc.
House Homeland Security Committee
Subcommittee on Cybersecurity and Infrastructure Protection
"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"
March 23, 2023

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 the Cybersecurity and Infrastructure Security Agency (CISA) and the state of American Cybersecurity.

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. 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. In collaboration with industry, government and academia, Tenable is raising awareness of the growing security risks impacting critical infrastructure and of the need to take steps to mitigate those risks. I also recently served as the staff lead under Tenable Co-Founder Jack Huffard in the development of the Report on Information Technology (IT)/OT Convergence Report[1] issued by The President's National Security Telecommunications Advisory Committee (NSTAC). Prior to joining Tenable, I worked in 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 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 CISA.

About Tenable

Tenable is headquartered in nearby Columbia, Maryland, and has 1,900 employees globally and approximately 43,000 customers worldwide. Tenable is publicly traded on the NASDAQ and is the world's leading provider of vulnerability management capabilities. We believe cybersecurity is foundational to making better and more strategic decisions. Our goal is to eliminate blind spots and help organizations prioritize which actions they can take to most efficiently reduce exposure and loss.

Tenable empowers organizations of all sizes to understand and reduce their cybersecurity risk. For the federal government specifically, Tenable provides the most widely deployed vulnerability management solution, serving just about every department and agency. Our solutions are also broadly used by state and local governments to manage cybersecurity risk.

---

[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

The Current State of OT/Critical Infrastructure/Federal Cybersecurity

Over the past few years, we have seen a dramatic increase in the frequency of successful cyberattacks against U.S. public- and private-sector organizations and have experienced new threats targeting our critical infrastructure. New ransomware and extortion groups routinely exploit known vulnerabilities to gain access into organizations, with at least 31 new groups discovered from November 2021 to October 2022, resulting in ransomware attacks intensifying, exposing reams of data and accounting for over 35% of data breaches.[2]

In February 2021, a water treatment plant in Oldsmar, Florida, was breached when attackers attempted to poison the water supply.[3] Just months later, a ransomware attack against Colonial Pipeline shut down operations for six days, prompting the President of the United States to issue a state of emergency.[4] Following Russia's invasion of Ukraine last year, and increased threats of malicious activity against the U.S. and our allies, CISA and other law enforcement agencies took swift steps to warn governors, public sector partners and critical infrastructure providers to harden their cyber defenses, including through the "Shields Up" initiative.[5]

Just this month, a breach of D.C. Health Link, the health insurance exchange which serves members of Congress and their staff, resulted in the online exposure of personal data of more than 56,000 customers.[6] While unfortunate, this breach is not surprising as healthcare was the No. 1 sector targeted by ransomware attacks last year with 472 breaches, followed by the public administration sector, which includes governments, towns, and municipalities with 162 breaches.[7]

When it comes to reducing cyber risk, organizations worldwide find themselves restricted by deeply entrenched people, process and technology issues. An orientation toward reactive, incident-focused cybersecurity practices means preventive tasks are often relegated to nothing more than a compliance exercise. Teams are measured by how many vulnerabilities they've remediated, rather than by how effectively they've reduced their organization's exposure.

The siloed nature of cybersecurity, especially between IT and OT teams — each with their own, sometimes contradictory, goals — exacerbates the problem. It is nearly impossible for cybersecurity leaders to obtain a unified and contextual view of their exposure using the existing tools at their disposal. The processes involved — which often require cybersecurity teams to convince their counterparts in IT, cloud and Development Operations (DevOps) to take necessary security precautions

---

[2] Tenable, "2022 Threat Landscape Report," https://static.tenable.com/marketing/research-reports/Research-Report-2022_Threat_Landscape_Report.pdf

[3] ABC News, "Florida city's water treatment system hacked by 'intruder,' investigators say," https://abcnews.go.com/US/florida-citys-water-treatment-system-hacked-intruder-investigators

[4] NPR, "What We Know About The Ransomware Attack On A Critical U.S. Pipeline," https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline

[5] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Shields Up," https://www.cisa.gov/shields-up

[6] Roll Call, "House, Senate members affected in DC Health Link breach to total 21," https://rollcall.com/2023/03/14/house-senate-members-affected-in-dc-health-link-breach-total-21

[7] Ibid 2.

— are fraught with opportunities for error and conflict. The siloed nature of the many preventive security tools offered by cybersecurity vendors means there's no way to determine how much exposure any given weakness actually represents at any given time. The reason? Security pros using siloed tools are unable to determine the relationships among users, systems and software. Without a unified and contextual view of their environments, security professionals cannot realistically identify the objective security truths that indicate their exposure to risk.

These issues are not new. While applying basic cyber hygiene can reduce exposure, it's long been challenging for organizations to achieve with existing preventive tools. What is new is the expanding complexity of the modern attack surface. Modern IT infrastructure encompasses multiple cloud systems, numerous identity and privilege management tools, multiple web-facing assets along with operational technology (OT) and internet of things (IoT) systems and software.

Today's IT environment brings with it numerous opportunities for misconfigurations and overlooked assets. The lack of a unified and contextual view of users, systems and software means security teams cannot effectively evaluate what's happening across the attack surface. And competing business interests often mean speed and uptime are favored over security.

Government officials and private sector leaders are paying increasing attention to critical infrastructure vulnerabilities, particularly those brought on by the convergence of IT and OT technologies. Since the late 1960s, OT has been part of manufacturing, utilities and other critical infrastructure sectors, and has been considered technology "safe" from attacks because most OT devices were not connected to outside networks. However, in today's modern facilities, these devices are no longer air-gapped and are now in many cases exposed to the internet — and to the threat of cyberattacks.[8]

The combination of IT and OT systems makes OT systems susceptible to the same risks of malware and threats that IT systems face today. Between the two: OT has different performance requirements than IT; OT systems serve a specific purpose while IT systems serve a wide variety of technologies; and OT systems have a lifecycle of a decade or more while IT systems are much shorter. This creates different priorities between IT security professionals and OT system operators within organizations. While IT security practices can inform OT security requirements, the OT systems require more specialized solutions which address the performance requirements of the system.[9]

Securing IT and OT systems and their convergence has become a national security imperative. Public-private sector collaboration to address cyberthreats is essential to building resilient and robust converged IT/OT environments. CISA is the national coordinator for critical infrastructure security and resilience and, as the Administration's National Cybersecurity Strategy emphasizes, it must enhance strategic collaboration and scale public-private partnerships in favor of greater security and resiliency.[10]

Given the heightened threat landscape, CISA and Congress have started to recognize the need to prioritize critical infrastructure security and have begun making much-needed investments. CISA is

---

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

[9] President's National Security Telecommunications Advisory Committee, "Information Technology and Operational Technology Convergence Report," https://www.cisa.gov/sites/default/files/publications

[10] The White House, "National Cybersecurity Strategy," https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

working to guide the nation's state and local governments, critical infrastructure providers and other private sector organizations, and federal entities, to strengthen their cyber defenses. In Congress, the House Committee on Homeland Security led efforts to include a $1 billion state and local cybersecurity grant program in the Infrastructure Investment and Jobs Act. The program will help state, local, tribal and territorial governments safeguard these vital systems from future attacks.

CISA 101

CISA was established on November 16, 2018, to defend and secure our nation's cyberspace and build a resilient and robust critical infrastructure for the American people. As a relatively new federal agency, CISA has made strides in elevating cybersecurity and infrastructure security as national security issues. Unlike other well-established federal organizations, CISA is working at start-up speed to keep American organizations ahead of growing and constant cyberthreats.

There has been significant activity under Director Jen Easterly's leadership to strengthen the U.S. cyber posture, including prioritizing public-private partnerships, developing new cybersecurity initiatives and implementing cybersecurity policies proposed by Congress and the Administration.

Joint Cyber Defense Collaborative (JCDC)

CISA established the Joint Cyber Defense Collaborative (JCDC) to lead "integrated public-private sector cyber defense planning, cybersecurity information fusion, and dissemination of cyber defense guidance to reduce risk to critical infrastructure and National Critical Functions."[11] Tenable is a proud Alliance Partner of the JCDC, which has enabled us to collaborate with CISA across a range of cybersecurity issues and challenges, to provide strategic insights and operational response acumen. 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. In fact, known vulnerabilities dating as far back as 2017 were so prominent in Tenable's 2022 Threat Assessment Report findings that they occupied the top spot in the 2022 list of the top 5 vulnerabilities.[12]

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Following passage and implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CISA began development of cyber incident reporting regulations as required by the new law.[13] Timely cyber incident reporting – both from critical infrastructure entities to CISA and from CISA to its industry stakeholders – enables rapid identification, remediation, and proactive defense against these and similar incidents. CISA's commitment to working with industry stakeholders to develop thoughtful, effective, and balanced reporting requirements will further strengthen the cybersecurity of our nation's critical infrastructure.

As part of the regulatory development process, Tenable provided CISA with input as the agency developed its cyber incident reporting regulations required by CIRCIA. Among its input, Tenable proposed the following three primary recommendations to effectively improve threat and incident situational awareness:

---

[11] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Joint Cyber Defense Collaborative," https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet_508C.pdf

[12] Ibid 2.

[13] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),"https://www.cisa.gov/topics/cyber-threats-and-advisories

1. That CISA request contextual details about the specific vulnerability exploited in the cyber incident and actionable information about the nature of the incident, including tactics, techniques, and procedures (TTPs), and indicators of compromise (IOCs).
2. That CISA share this information, utilizing the traffic light protocol with a trusted group of cybersecurity stakeholders, such as JCDC Alliance Partners.
3. That actionable information sharing across the critical infrastructure sectors would enable owners and operators to help defend their organizations against and respond to cyberattacks.

Binding Operational Directives (BOD)

CISA also has authority to issue Binding Operational Directives (BOD), which are compulsory directions to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.[14] In 2021, CISA issued BOD 22-01, which requires federal agencies "to remediate vulnerabilities in the KEV catalog within prescribed timeframes."[15] The Known Exploited Vulnerabilities (KEV) catalog is maintained by CISA and helps organizations prioritize remediation of listed vulnerabilities and reduce the opportunities for threat actors to compromise systems.

Following recommendations to conduct asset inventories of OT systems included in last year's NSTAC Report to the President, CISA issued BOD 23-01 to require federal agencies to improve asset visibility and vulnerability detection on federal networks.[16] To provide additional visibility into the variety of assets that make up the modern attack surface and help agencies understand the full scope of their cybersecurity risk, BOD 23-01 mandates continuous and comprehensive asset visibility. The BOD focuses on two core activities that are essential to maintaining a successful cybersecurity program:

- Asset discovery
- Vulnerability enumeration

By mandating continuous and comprehensive asset visibility, BOD 23-01 will ensure that federal agencies have the necessary foundation to maintain a successful cybersecurity program.

This directive applies to all IP-addressable networked assets that can be reached over IPv4 and IPv6 protocols. It builds on BOD 22-01 and outlines new requirements for cloud assets, IPV6 address space, and operational technology (OT) in an effort to reduce cyber risk.

Cross-Sector Cybersecurity Performance Goals (CPGs)

In 2021, the Biden Administration issued the National Security Memorandum on Improving the Cybersecurity for Critical Infrastructure Control Systems, outlining initiatives in the electricity, pipeline, water, and chemical sectors, and calling for the development of cross-sector cybersecurity performance goals for critical infrastructure.[17]

Last October, CISA released its Cross-Sector Cybersecurity Performance Goals (CPGs), based on relevant categories and subcategories of the NIST Cybersecurity Framework (CSF), to address some of the nation's

[14] 44 U.S.C. § 3552(b)(1). U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Binding Operational Directive 23-01," https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01

[15] 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

[16] Ibid 9.

[17] The White House, "National Security Memorandum on Improving the Cybersecurity for Critical Infrastructure Control Systems," https://www.whitehouse.gov/briefing-room/statements-releases

most frequent and impactful cybersecurity risks. The CPGs also emphasize OT security and how it is often overlooked and under-resourced.[18] By offering IT/OT cybersecurity guidance, CISA's CPGs create a baseline set of cybersecurity practices and benchmarks for critical infrastructure operators to measure and improve their cyber posture. Earlier this week, CISA released stakeholder-based updates to the CPGs that are more strongly aligned with the functions, categories, and subcategories of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is widely utilized by critical infrastructure owners and operators and the greater alignment of the CPGs will make them more accessible to these entities.

Pillar One of the Administration's new National Cybersecurity Strategy builds on this notion of establishing cybersecurity best practices and expanding the use of minimum cybersecurity standards, such as the adoption of basic cyber hygiene and secure-by-design principles. This reinforces that IT/OT convergence will continue to be a security issue for years to come, and organizations need a plan to address these challenges.[19]

Tenable was pleased that CISA incorporated input from multiple critical infrastructure industry stakeholders, including relevant sector coordinating councils (SCCs) in the development of the CPGs, ensuring they were aligned with the NIST CSF. We are also encouraged to see the Administration emphasize similar approaches to mitigate cybersecurity risk in its National Cybersecurity Strategy. Baseline cybersecurity requirements or standards of care for critical infrastructure, which align with CISA's Cross-Sector Cybersecurity Performance Goals, international standards, and the NIST CSF, drive better cybersecurity and a more resilient ecosystem.

Secure-by-Default

In recent months, CISA has spearheaded efforts to shift the security burden from consumers to putting the onus on manufacturers to ensure built-in security is a feature of all technology products, especially those that support critical infrastructure. Director Easterly stated, "the leaders of technology manufacturers should explicitly focus on building safe products, publishing a roadmap that lays out the company's plan for how products will be developed and updated to be both secure-by-design and secure-by-default."[20] Likewise, CISA launched the Ransomware Vulnerability Warning Pilot program to help identify vulnerabilities in critical infrastructure systems and inform owners to take action before a potential cybersecurity incident occurs.[21] In conjunction with the other initiatives CISA has developed, these efforts will work to advance the nation's cybersecurity resiliency.

Separation of Duties / Independent Assessments of Software

Similar to the Sarbanes-Oxley Act of 2002 requirement for firms to separate their auditing function from their consulting function, "separation of duties" in cybersecurity is necessary to prevent conflicts of interest, misaligned incentives, and increased security risks. The U.S. Securities and Exchange Commission states that an auditor is not capable of exercising objective and impartial judgment if a

[18] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[19] The White House, "National Cybersecurity Strategy," https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[20] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "The Cost of Unsafe Technology and What We Can Do About It," https://www.cisa.gov/news-events/news/cost-unsafe-technology-and-what-we-can-do-about-it
[21] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "CISA Announces Ransomware Vulnerability Warning Pilot," https://www.cisa.gov/news-events/alerts/2023/03/13

relationship with or service provided by an auditor "(a) creates a mutual or conflicting interest with their audit client; (b) places them in the position of auditing their own work…"[22]
CISA should apply the Sarbanes-Oxley "separation of duties" principles to cybersecurity and prohibit the provider responsible for developing and/or running software programs from also testing its security, conducting security audits, or reporting on its security.

What's Next: CISA 2025
CISA has worked to enable organizations and critical infrastructure providers to understand, manage, and reduce their cybersecurity risks, but there is still much work to be done. Naturally, as the agency evolves, there is a significant need for continued improvements to strengthen our cybersecurity efforts and to address the many unique needs of the critical infrastructure sectors.

While some of the 16 identified critical infrastructure sectors[23] have a high degree of cybersecurity preparedness, strong risk understanding and risk management practices, and very strong security programs, others are woefully ill prepared. New technology investments represent great efficiency opportunities, like the move to smart factories and smart cities, but these shifts can introduce real gaps in security. Continued digital transformation, increasingly interconnected IT and OT systems, and an expanding cyberattack surface will require enhancements to security and resiliency. Critical infrastructure providers must be prepared to address tomorrow's cyberthreats and it is CISA's responsibility to support them in that effort.

Zero Trust Architecture
The White House issued a Federal Zero Trust Architecture (ZTA) Strategy in January of 2022, requiring agencies to implement Attack Surface Management (ASM) as part of their ZTA by the end of fiscal year 2024. The memorandum states, "to effectively implement a zero trust architecture, an organization must have a complete understanding of its internet-accessible assets so that it may apply security policies consistently and fully define and accommodate user workflows."[24] ASM enables organizations to identify assets and look for vulnerabilities from the outside in, from the attacker's perspective, and will give agencies complete asset discovery, increase awareness of what is on their networks, and improve vulnerability management.

The memorandum further states, "for agencies to maintain a complete understanding of what internet-accessible attack surface they have, they must rely not only on their internal records, but also on external scans of their infrastructure from the internet."[25] Ultimately, organizations cannot take a 'trust no one' approach on a device if they do not know the device exists; however, ASM enables that visibility.

As agencies look to comply with the White House's ZTA strategy by moving towards a zero trust architecture and taking a 'trust no one' approach to security, the security of an agency's underlying user identity and privilege management system itself comes into play. To ensure identity systems are secure, agencies need to be able to identify everything in their complex Active Directory (AD) environment,

[22] The U.S. Securities and Exchange Commission, "Audit Committees and Auditor Independence," https://www.sec.gov/oca/audit042707
[23] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[24] The White House, "Federal Zero Trust Architecture (ZTA) Strategy," https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[25] Ibid 24.

predict what matters to reduce risk, and eliminate attack paths before attackers exploit them. Effective management of AD users and privileges allows agencies to take a proactive approach to address and mitigate future cyberthreats.

NSTAC IT/OT Convergence Report

In response to growing cybersecurity threats to the critical infrastructure upon which Americans depend, the White House tasked The President's National Security Telecommunications Advisory Committee (NSTAC) with conducting a multi-phase study on "Enhancing Internet Resilience in 2021 and Beyond."[26] The Subcommittee for the second phase of the study was charged with developing the NSTAC Report to the President on IT/OT Convergence.[27] I co-led the subcommittee's working group to produce this report. The report identifies three opportunities for the federal government:

- to help relevant stakeholder communities execute a secure convergence of IT and OT cybersecurity;
- to examine the key challenges of securing converged OT systems against threats that emerge from IT network connections; and
- to identify emerging approaches to increase OT resiliency to these threats

The subcommittee received briefings from more than 30 subject matter experts across government and private industry. First, the subcommittee heard from government owners and operators of OT systems and policymakers focused on IT and OT cybersecurity; second, we heard from critical infrastructure owners and operators of converged IT/OT environments and original equipment manufacturers; and third, we heard from cloud service providers, integrators, and cybersecurity vendors.

NSTAC Report Findings

On August 23, 2022, NSTAC approved the Report to the President. The report findings revealed several consistent themes highlighting that the convergence of IT and OT systems is not a new issue. As a nation, we have not prioritized securing IT/OT interconnected systems, despite having the technology and knowledge readily available. Even in 2022, the report found organizations lack visibility into their OT environments, which is exacerbated by the traditional silos within which OT and IT personnel operate. The current siloed approach demonstrates a need to promote harmonization through a unified structure to better manage shared responsibility to secure converged environments.[28]

Stakeholders also rarely take the opportunity to proactively "build in" security where appropriate and opt instead to "bolt-on" security in OT environments after the fact, costing organizations valuable time and resources to recover from cyber incidents and unpatched vulnerabilities.

Businesses, organizations, and governments need to share the responsibility of building a more sustainable cybersecurity model to create ecosystems that take a secure-by-design approach to ensure the long-term cybersecurity resiliency of our country - a point Director Easterly and CISA Executive Director Eric Goldstein recently emphasized.[29]

---

[26] President's National Security Telecommunications Advisory Committee, "NSTAC Fact Sheet,"https://www.cisa.gov/resources-tools/resources/presidents-nstac-fact-sheet
[27] Ibid 9.
[28] Ibid 9.
[29] Foreign Affairs, "Stop Passing the Buck on Cybersecurity," https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity

NSTAC Recommendations to Improve Critical Infrastructure Security
Based on the findings, the subcommittee developed 15 presidential, strategic, and actionable recommendations to address the many concerns expressed to the subcommittee through the briefing phases. Amongst the 15 recommendations, the subcommittee identified three consequential recommendations for the President to strengthen the cybersecurity posture of U.S. government owned and operated OT systems that should be prioritized.

The report first recommends that CISA 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), that requires 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, including an understanding of any interconnectivity to other systems. An up-to-date inventory should be required as part of each department's or agency's annual budget process.

Once federal agencies clearly understand the vast and interconnected nature of their OT devices and infrastructure, they can then make risk-informed decisions about how to prioritize their cybersecurity budgets to best protect the most consequential of those assets.

Second, CISA should develop guidance on procurement language for OT products and services, and for products and services that support converged IT/OT environments, to incentivize the inclusion of risk-informed cybersecurity capabilities, including for supply chain risk management. This guidance should also help organizations understand best practices for bolt-on security for legacy OT devices that are difficult or expensive to replace.

CISA should work with the General Services Administration (GSA) to require the inclusion of risk-informed cybersecurity capabilities in procurement vehicles for the federal government. There should also be a mechanism for both private sector users of the procurement guidance and public sector agencies, which must follow the new requirements, to provide feedback and lessons learned to aid the community.

Finally, the NSC, CISA, and the Office of the National Cybersecurity Director (ONCD) should prioritize developing and implementing interoperable, technology-neutral, vendor-agnostic information-sharing mechanisms to enable real-time sharing of sensitive collective-defense information between authorized stakeholders involved with securing U.S. critical infrastructure. This should include breaking down the artificial barriers for sharing controlled unclassified information, both within the U.S. government and between government and other key, cross-sector stakeholders.

Additional recommendations in the report to secure U.S. OT infrastructure call on CISA and the ONCD to clearly articulate roles and responsibilities for federal agencies that support critical infrastructure and other industry stakeholders. Concurrently, CISA should work with the Office of Management and Budget (OMB) to develop key IT/OT convergence cybersecurity performance indicators and implementation timelines for agencies and hold agency heads accountable. Furthermore, the ONCD, in partnership with CISA, should facilitate an interagency study that evaluates conflicting regulations for OT operators to identify opportunities to streamline OT cybersecurity regulation.

Based on the subcommittee briefings, it was evident that the federal government has historically underfunded OT cybersecurity. Fortunately, the Infrastructure Investment and Jobs Act (IIJA) has created

numerous grant programs that include cybersecurity as an allowable expense, presenting an opportunity for the ONCD and CISA to collaborate with Sector Risk Management Agencies (SRMA) to ensure that cybersecurity is a priority item in any grant application. Of note, the State and Local Cybersecurity Grant Program (SLGCP) appropriates $1 billion in grant funding over the next four years to help advance OT cybersecurity. Tenable has been leading efforts to educate eligible entities on how to apply for grant funding and implement cybersecurity solutions that address the growing threats and risks to their information systems.[30]

Binding Operational Directive 23-01

As previously mentioned, last October CISA issued Binding Operational Directive (BOD) 23-01, calling on federal civilian departments and agencies to "make measurable progress toward enhancing visibility into agency assets and vulnerabilities," aligning with NSTAC's IT/OT Convergence Report recommendations.[31]

BOD 23-01 mandates continuous and comprehensive asset visibility, focusing on two core activities essential to maintaining a successful cybersecurity program: asset discovery and vulnerability enumeration. According to BOD 23-01, "continuous and comprehensive asset visibility is a basic precondition for any organization to effectively manage cybersecurity risk. Accurate and up-to-date accounting of assets residing on federal networks is also critical for CISA to effectively manage cybersecurity for the Federal Civilian Executive Branch (FCEB) enterprise."[32] Federal agencies need comprehensive visibility into their assets and vulnerabilities across their organizations to protect against external unknowns.

Enumerating OT assets, critical infrastructure and vulnerabilities present unique challenges to federal agencies. 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 FCEB systems and agencies operating those systems meet said requirements, Congress should appropriate funding to implement CISA's BOD 23-01, enabling 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 as well as IT assets.

Policy Recommendations

Congressional action should not allow for "learned helplessness" by federal government agencies or private industry. There is too much at stake for individuals and organizations to remain negligent and not take even the most basic steps to improve their cyber posture..

Tenable recommends the following steps that Congress should implement to enhance the cyber preparedness of U.S. critical infrastructure:

---

[30] H.R.3684 – 117th Congress (2021-2022): Infrastructure Investment and Jobs Act. (2021, June 4). https://www.congress.gov/bill/117th-congress/house-bill/3684/text

[31] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Binding Operational Directive 23-01," https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01

[32] Ibid 31.

- **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, scanning for and patching known vulnerabilities, and implementing incident detection and response capabilities. 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.

- **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; will request and share anonymized data on the types of vulnerabilities that were exploited and the attack paths that adversaries followed after infiltrating target networks; and provides actionable information through trusted partners, such as JCDC Alliance Partners, to provide cyber situational awareness to the broader critical infrastructure ecosystem to enable entities to protect themselves against ongoing and potential attacks.

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

- **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 the serious risk. 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 requests for proposals and procurement processes seldom 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 and 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, in a standardized, technology-neutral way, in order to leverage cyberthreat and vulnerability information from the broader critical infrastructure ecosystem.

- **Ensure CISA and FCEB agencies are adequately resourced to implement BOD 22-01 and BOD 23-01 policy recommendations.** Protecting our nation's cybersecurity means knowing what's on our networks and maintaining it 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 scan 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

- **Ensure sufficient funding for CISA and the Office of the National Cyber Director to ensure they can meet mission requirements.** Our company supported the creation of the Office of the National Cyber Director and applauded efforts to stand up and staff the new office. 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. Congress should see the FY 2024 appropriations for CISA as a new baseline number, which should grow at a rate commensurate with the needs of the mission.

- **Support and strengthen value added engagement between the private sector and public sector**. The JCDC, of which Tenable is a member, is bringing together representatives from private industry and key government agencies to drive strategic planning and incident response capabilities. This type of operational government-industry engagement has been a positive step forward and we urge Congress to continue supporting and strengthening the JCDC's alignment.

- **Accelerate deployment of Zero Trust including Active Directory and Attack Surface Management.** Congress should provide federal agencies with the resources needed to implement Cyber Executive Order 14028 to modernize and strengthen our collective cyber defenses, recognizing that Zero Trust is a philosophy that dictates systems design and operation, not a singular product.
    - **All government systems must incorporate Active Directory security** to ensure least privileges for user identities, and to scan for misconfigurations that can be exploited to gain access to Active Directory and monitor for ongoing suspicious and high-risk activities within Active Directory.[33]
    - **Attack Surface Management,** which continuously scans the internet to discover, inventory, classify, and monitor an organization's IT infrastructure, **will give agencies**

[33] U.S Department of Commerce, "NOAA Inadequately Managed Its Active Directories That Support Critical Missions," https://www.oig.doc.gov/OIGPublications/OIG-22-018-A.pdf

complete asset discovery, increase awareness of what is actually on their networks, and will improve vulnerability management.

Conclusion

There are fundamental steps all federal agencies and critical infrastructure sectors must take — from knowing what's on their network and how those systems are vulnerable to addressing known exposures, and from controlling user access and privileges to managing critical systems that are interconnected — that will make it harder for bad actors to compromise interconnected IT and OT systems.

Many critical operating environments lack a formal systemic approach to risk assessments and processes, let alone the continuous visibility expected for critical services and high value targets. These formal processes are desperately needed as rapid increases in access and interconnectivity dramatically increase risk**.** In these instances, policy guidance for transparency and standards of care can help drive improvements in risk management practices and at the same time foster innovation.

Thank you Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and members of the Subcommittee for your attention to these important issues and continued assessment of the work CISA is doing to keep Americans safe. I appreciate the work this committee is doing to elevate cybersecurity with bipartisan support. Thank you for the opportunity to testify today and I look forward to working with you to secure our nation's cyber assets.