CYBER STATECRAFT
INITIATIVE

#ACcyber

ISSUE BRIEF

JULY 2024

OT Cyber Policy: The Titanic or the Iceberg?

DANIELLE JABLANSKI

EXECUTIVE SUMMARY

The maritime sector is both a commercial and defense industry, critical economically and for national security. Although the *Titanic* was primarily a passenger vessel, it also carried a substantial amount of cargo. Ships, once primitive, transformed into analog marvels of engineering, then into highly digitized floating systems of systems. Some rival small cities, with complex interdependent systems and supply chains for things like power, sanitation, food, communication, navigation, medicine, healthcare, and retail.

However, manufactured vessels still seem like a commodity item, like any other raw material. Despite potential malfunction or mishap, manufacturers do not own and operate commercial ships once they leave the port, so their (vendor) liability and support depend on each component, contract, and situation. What is not fully managed or entrusted to owners and operators is outsourced to third parties, with checks and balances further delegated to laws, regulations, compliance, and insurance.

Today, cyber-physical operations across critical infrastructure are treated as both the *Titanic*–a complex system of interdependent digitized systems–and the iceberg, as many people refer to a speculative “cyber 9/11” or “cyber–Pearl Harbor.” Deploying dual-use technology, all sixteen critical infrastructure sectors in the U.S. impact civilian life and national security. Inherently, however, control systems–known as operational technology (OT) or industrial control systems (ICS)–are owned and operated vendor products with responsibility for their security shared by many different stakeholders.

Current policy does not address the issue of cyber-physical security with a systemic approach, instead focusing with tunnel vision on specific events, such as demonstrated adversarial capabilities, discovered vendor product vulnerabilities and patches, or patterns like USB attacks This reactionary impulse makes prioritization difficult across sectors, entities, and their critical functions. Generally, organizations and agencies cannot reasonably determine where the highest concentration of vulnerable or homogenous systems are deployed, nor which entity will be targeted next.

This dynamic has resulted in a general “Shields Up” stance, but a lack of prioritization, among the sixteen critical infrastructure sectors and a plethora of efforts to con-

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

textualize and address the growing concerns for cyber-physical systems, which only tackle parts of the problem. Furthermore, stakeholders across critical infrastructure struggle to discern the potential impacts on the integrity of their systems and processes of each attack scenario, to prioritize actions and activities, and to calculate the cost-benefit analysis of those actions and activities.

This issue brief illustrates why no one-size-fits-all approach is appropriate for OT cybersecurity, and how each stakeholder has a role to play in enhancing the security of cyber-physical systems, including vendors, owners and operators, and national security and defense practitioners and policymakers. Borrowing again from the *Titanic* analogy, this analysis uses the iceberg model for systems thinking to address policy gaps existing between the various levels of the OT ecosystem, detailing the following recommendations for the Cybersecurity and Infrastructure Security Agency (CISA):

1. Streamline available OT and industrial controls systems (ICS) cybersecurity data
2. Align public-private risk researchers and analysts
3. Conduct Cyber Performance Goal (CPG) reviews with low, mid, and high-maturity organizations
4. Expand training and awareness

INTRODUCTION

The general public clearly believes the US government has a key role to play in securing and maintaining infrastructure that underpins economic and national security. Survey data released by the MITRE Corporation in March 2024 reveals that 49 percent of the public believes the federal government bears partial responsibility for fortifying critical infrastructure. 29 percent believe the federal government is solely responsible.[1] Despite its central role, however, the federal government currently lacks the data and resources to prioritize where and how to secure and fortify OT and ICS networks across the nation and its many sectors and interdependent global supply chains.

A primary cause of this problem is that federal cybersecurity policymakers, sector risk management agencies (SRMAs), and research and development teams lack a holistic understanding of critical operational technology and industrial control systems, as well as the risks of cascading cyber-physical impacts. Despite the barrage of recent frameworks, assessments, and recommendations to coalesce the field around shared principles and security controls,[2] cybersecurity is inherently subjective. Each asset owner's unique perspectives and needs determine its priorities. Similar concerns exist across industries, but heterogeneous systems, configurations, and networks do not result in homogeneous risks, impacts, or outcomes.

A secondary cause of this problem is that available datasets and information-sharing regimes for OT and ICS vulnerabilities and threat intelligence are siloed, resulting in limited sampling for cyber-physical environments—limited by the number of participating asset owners, sector coverage, available indicators of compromise, and national security clearance measures. This creates multiple single sources of information without much consensus. Despite this variation, however, OT systems do have some common characteristics that are vital for cybersecurity experts to understand.

OT SYSTEMS BACKGROUND: DEVICES, NETWORKS, AND ACCESS

Operational technology is a broad set of technologies covering process automation, instrumentation, cyber-physical operations, and industrial control systems (ICS). OT systems are often connected to other supervisory control and data acquisition (SCADA) systems and field devices or instrumentation, with control data separately captured for use in business applications. Operational technology can be found in a variety of contexts, from control systems that automatically run assembly lines and manufacturing processes to those that produce and deliver electricity, lighting, and heating.

Regardless of the context, all sectors with OT systems have three things in common: critical assets (machines and equipment essential to operations), critical functions (processes and outputs of operations), and varying cyber risk and exposure. However, risks to OT and ICS do not apply to all systems in the exact same way. OT and ICS systems are built with significant protocol and configuration differences, which are often customized for their intended purpose, presenting competing demands for availability, safety, and security priority and attention.

After infecting an intermediary system, a threat actor or group of actors may pivot into control networks either in a supervisory capacity (read-only) or with the ability to send commands (write) to control systems that dictate instructions to field devices that move, turn, heat, cool, open and close physical devices in the real world. Without personnel manually responsible for the functioning of all the turbines, pumps, valves, actuators, dials, and cyber-physical processes, it is virtually impossible for owners and

[1] "Public Perceptions on Security Critical Infrastructure," MITRE, March 2024, https://www.mitre.org/focus-areas/cybersecurity/public-perceptions-securing-critical-infrastructure.

[2] "Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World," President's Council of Advisors on Science and Technology, February 2024, https://www.whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.

operators to disconnect these vital systems from their intermediary counterparts and principal business requirements.

Many of these systems—which are often designed to last fifteen years or more—inherently lack encryption, password protection, multifactor authentication, and other best practices for cybersecurity. Some systems only allow for short windows of time—sometimes only 24 to 48 hours offline—to install critical software patches. Due to this difficulty, owners or operators often opt to harden systems instead of isolating, securing, patching, or replacing an insecure device. Hardening devices is a practice that requires configuration changes to disable or remove any services or programs not required for normal or intended system operations. Reducing the number of services and programs removes superfluous access and frivolous data exchange, lowering the number of potentially exploitable attack paths.

There are thousands of known software and application vulnerabilities from each vendor that manufactures machinery and equipment. Although vulnerabilities are published with an associated common vulnerability score, the rating is specific to the vulnerability in the system itself and does not translate to the severity of the vulnerability in the context of a deployed environment. Vulnerabilities must be analyzed in the context of their operations to understand their significance and prioritize remediation and response efforts.

It is incredibly challenging to manually verify the exposure or risk status of numerous operational devices at all times. There are many reasons for this, including a lack of system provenance, supply chain and chain of custody issues, and limited root cause analysis capabilities. If an owner or operator cannot entirely secure its network, it must reinforce it with access controls—both machine to machine and user or role-based interactions. If authentication is not possible or credentials can be spoofed or bypassed, teams will then need to harden devices. And if OT devices are vulnerable or no longer supported by their vendor, network security remains a top priority. This cycle repeats asset by asset, process by process, network by network, and company by company.

When examining OT vulnerabilities, cybersecurity conversations sometimes overlook the physical layer of protections often built into control systems, called interlocks. These protective physical and logical components "define mutually exclusive conditions to prevent undesired (harmful) states of the process" such as acceptable voltage, chemical levels, or speed parameters.[3] Focusing solely on the cyber aspects of control systems and their connectivity overlooks the complexity of this physical protection logic and disproportionately focuses attention on systems or controls that may not reduce risk.

Thus, policy solutions to improve OT cybersecurity largely fall into two camps. The first focuses on securing or replacing the control system equipment or systems, while the second focuses on avoiding cyber incidents altogether by promoting risk avoidance, security controls, and best practices; often relying on a single motivating event or threat actor for urgency. With limited resources, including budgets, personnel, and time, both these approaches have their drawbacks. Focusing on addressing product vulnerabilities is a cumbersome process that may not be financially or technically viable. Focusing on avoiding all cyber risks, on the other hand, often ignores the importance of different critical assets and their essential functions.

CONNECTING CRITICALITY AND "CYBER"

The numerous challenges of securing OT and ICS in the current context pose a natural question: if the critical infrastructure US citizens need to maintain their quality of life—clean water, sanitary hospitals, safe and reliable electricity, critical manufacturing, and more—is so vulnerable to cyberattack, why not take it all offline? This question was asked by Congressman Carlos Gimenez during a February 2024 House Homeland Security Committee hearing on operational technology.[4] While the desire for a simple fix is understandable, this approach is unrealistic given the scope and scale of digital technologies for both localized and distributed operations.

Localized operations like regional or municipal utilities and multinational corporations like oil companies and automobile manufacturers cannot meet the demands of their businesses without relying on connected digital infrastructure. From logistics and scheduling to enterprise resource management, reliability, and process monitoring, typical IT and business systems rely on data from processes that are now automated via digital and network-connected technologies. These numerous technologies and systems are and will continue to be susceptible to cyberattacks.

In an attempt to prioritize critical services and functions, the congressionally mandated Cyberspace Solarium Commission created the following categories for Systemically Critical Designations:

1. The interruption of critical services, including the energy supply, water supply, electricity grid, and/or emergency

[3] Marina Krotofil, "Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle," https://67a8c4b4-678a-443b-bcfa-f1260e164991.filesusr.com/ugd/8efadc_0772cf53bffb46b0a64d219b563710c5.pdf?index=true.

[4] "Securing Operational Technology: A Deep Dive into the Water Sector," US House of Representatives Subcommittee on Cybersecurity and Infrastructure Protection, February 6, 2024, https://homeland.house.gov/hearing/securing-operational-technology-a-deep-dive-into-the-water-sector/.

services, that could cause mass casualties or lead to mass evacuations.

2. The perpetuation of catastrophic damage to the economy, including the disruption of the financial market, disruption of transportation systems, and the unavailability of critical technology services.

3. The degradation and/or disruption of defense, aerospace, military, intelligence, and national security capabilities.

4. The widespread compromise or malicious intrusion of technologies, devices, or services across the cyber ecosystem.[5]

Unfortunately, the attack surface does not end with these systemically critical categories of services and functions. Despite categorizing entities, goods, and services as "systemically critical," there is also no established way to prioritize and secure specific asset owners or targets based on potential OT and ICS cyber scenarios or cascading impacts. Lack of prioritization also leads to a lack of preparation. And lack of preparation leads to misunderstanding of tolerance–the capacity to endure continued subjection to something or an allowable amount of variation of a specific quantity, especially in the dimensions of a machine or part.

In OT and ICS, fault-tolerant system design–where a system continues to operate despite software or hardware failures–is a well understood aspect of functional safety and hazard analysis but is ill-defined for cybersecurity. Functionally, operators measure, train, plan for, analyze, and handle various failures: sensor failure, effector failure, computer hardware or software failure, operator failure, negligence, or accident. However, it is much more difficult to predict all possible cyber scenarios, events, or attacks that would lead to similar failures. As a result, stakeholders struggle to understand cascading cyber-physical impacts. Things like manual operations, redundancy, and isolated networks and facilities for operations all matter as much as the forensic artifacts of a cyber incident.

What cyber experts call resilience (the ability of systems to withstand adversity and recover quickly), operations experts call tolerance (the threshold at which systems can effectively and consistently deal with stressful situations). Policymakers are left to bridge that gap with flexible solutions to complex problems amidst a widely distributed risk management landscape. However, defining actual risk, perceived risk, and acceptable risk to date has been marketed as blanket cyber resilience with very little understanding of system tolerance.

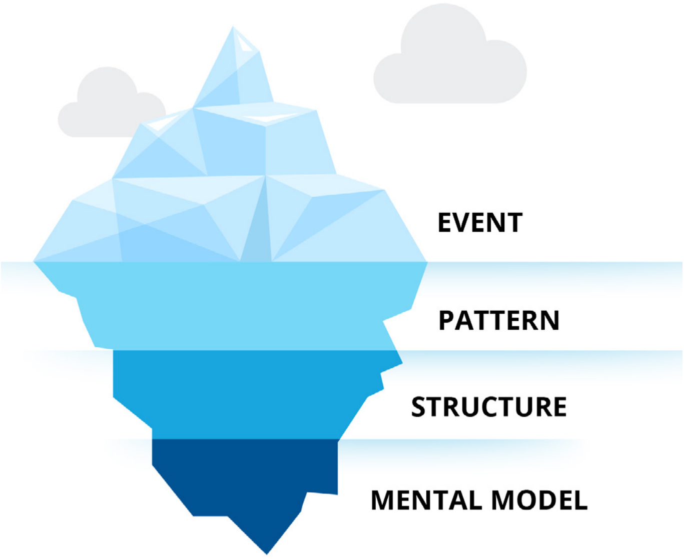
For instance, internet-connected devices may be hardened or have compensating security controls in place, representing a lower risk to organizations taking these steps. Vulnerabilities may require human interaction or physical access for exploitation, reducing their widespread impacts. Some organizations keep alternate backup systems ready to implement if critical assets are targeted or degraded. Others rely on physical logic embedded in systems that would prevent worst-case scenarios from occurring in the process control systems themselves. Finally, many safety systems provide alerts on an unsafe operational status that may be caused by some cyber threats and scenarios.

Engineers and operators understand fault-tolerant system design and cybersecurity experts understand security controls, but few business and government leaders understand the overlap and the gaps. Tolerance is essential for business calculations including annualized loss expectancy, maximum tolerable downtime, and mean time to recover. Determining tolerance, however, is complicated by the fact that there is no single definition of an OT cyber incident. Does the root of an incident have to be intentional, or could one also result from user error, negligence, or accident? Does a piece of OT or SCADA equipment or machinery need to be directly impacted to count? Many stakeholders have a role to play in determining and defining the extent of an incident.

[5] Tasha Jhangiani and Graham Kennis, "Protecting the Critical of Critical: What Is Systemically Important Critical Infrastructure?" *Lawfare*, June 15, 2021, https://www.lawfareblog.com/protecting-critical-critical-what-systemically-important-critical-infrastructure.

THE ICEBERG MODEL FOR SYSTEMS THINKING[6]

An iceberg represents a potentially catastrophic scenario—a situation commonly referring to something menacing or a harbinger of bad outcomes. Used as an idiom, the phrase "tip of the iceberg" often refers to some small, visible part of a much larger situation or context. Colliding with an iceberg, real or metaphorical, results in cascading impacts. This logic forms the basis of the "iceberg model" for systems thinking, which businesses, policymakers, and academics use to critically evaluate problems in complex ecosystems. The tip of the iceberg, called "the event," is the most visible activities that occur within a system. The iceberg model, however, is designed to push thinking beyond the most obvious symptoms into further levels of "patterns," "structures," and "mental models." When it comes to security for cyber-physical operations, industrial control systems, and operational technology, potential zero-day incidents and malign nation-state actors really do represent just the tip of the iceberg.



At the event level of OT cybersecurity, vendors, owners and operators, and national security policymakers focus their efforts on addressing recent attacks, ransomware, espionage campaigns, zero-day vulnerabilities, and other high-profile developments. Below that, at the pattern level, more technical stakeholders look to address events taking place over time, like the vulnerabilities of control systems intentionally or inadvertently connected directly to the internet or advanced persistent threats (APTs) and their tactics, techniques, and procedures (TTPs) targeting remote or physical access.

At the structure level, OT environments are underpinned by legacy devices with vulnerabilities, flat networks, opaque patching policies, and unencrypted protocols. Original equipment manufacturers (OEMs) are primary actors at this level, investing in proprietary protocol design and development, and maintaining control and change authority over manufactured systems for various commercial and technical reasons. End users or asset owners exist between the pattern and structure segments, understanding the design and architecture of networks and facilities, and the contextual implications of cyber scenarios.

Threat researchers, intelligence analysts, and third-party security monitoring vendors exist between the event, pattern, and structure portions of the iceberg but are often overlooked in policymaking. They uniquely understand and quantify the risks of the potential exploitation of OT and ICS and networks deployed today. At the base of the iceberg is the mental model: the industry's established attitudes, beliefs, expectations, and values that are deeply rooted and difficult to change. For instance, this includes a reluctance to actively interrogate control systems (as opposed to passively) or the understandable hesitation to run IT scanning tools like Nmap to identify vulnerabilities in OT networks.

Core assumptions, market realities, conflicting priorities, budget and resource constraints, political will and capital, knowledge, awareness, and training all inform the belief system beneath OT cybersecurity and the schools of thought for how to address its many challenges. Blanket security requirements and compliance measures that do not account for the patterns, structures, and mental model struggle to cover the actual install base of OT and ICS vendor technologies, properly address the threat landscape, and contend with the unique potential for cascading impacts each asset owner faces.

OT policy today focuses on avoiding significant events, providing tools for pattern analysis, adding security requirements for OEMs and asset owners, and adding product and liability requirements for vendors at the structure level. Without connective tissue, these efforts will not lead to holistic outcomes that reduce risk and build resilience. A better approach to policymaking is to consider how policies, requirements, best practices, and compliance measures intersect and connect systemically to address cyber-physical risks, threats, and responsibilities for all stakeholders.

[6] "What are the benefits and limitations of the iceberg model for systems thinking?," LinkedIn, 2024, https://www.linkedin.com/advice/0/what-benefits-limitations-iceberg-model-systems.

POLICY GAPS

JD Work, Professor in the College of Information and Cyberspace at the National Defense University wrote, “Every time one sees an official advocating for a ransomware payment ban, the correct response is not to debate the policy failure modes that result from such a proposal. It is to call out that having failed to provide for the common defense…the state has left private enterprise with only two responses to predation.”[7] Despite the overwhelming amount of federal attention on critical infrastructure, many asset owners continue to feel like sitting ducks in the face of cyber threats due to this lapse.

Meanwhile, the United States and its allies are constantly assessing and reassessing offensive and defensive strategies in response to adversaries engaging in more provocative cyberattacks, like the Chinese-sponsored Volt Typhoon group’s attacks on the IT systems of critical infrastructure organizations and the evolution of more difficult-to-detect “living off the land” techniques. In short, the landscape for critical infrastructure cybersecurity is becoming more complex and confrontational, accentuating the shortcomings of the available solutions, protections, and investments in securing cyber-physical operations.

Where potential conflict red lines and theaters continue to blur, the 2024 Annual Threat Assessment of the US Intelligence Community from the Office of the Director of National Intelligence (ODNI) has doubled down on the fact that “China remains the most active and persistent cyber threat to the US government, private sector, and critical infrastructure networks,” and that “Russia maintains its ability to target critical infrastructure–including underwater cables and industrial control systems–in the United States as well as in allied and partner countries.”[8]

With any critical infrastructure organization a potential target, it is useful to review competing priorities in recent policy. Starting from a high level, the Biden administration announced its new National Cybersecurity Strategy (NCS) in March 2023 as a comprehensive approach to safeguarding US critical digital infrastructure. The strategy is composed of five pillars, of which the first and arguably most important for homeland security is “Defend Critical Infrastructure.” The Cybersecurity and Infrastructure Security Agency (CISA) is tasked with the subsequent functions in that pillar.[9]

With these functions in mind, CISA’s Cybersecurity Strategic Plan for FY2024-2026, published in August 2023, has three primary objectives as a subdivision of national cybersecurity priorities second to the NCS:

1. Address immediate threats

2. Harden the terrain

3. Drive security at scale[10]

“Operational technology” is mentioned three times in this strategy, though “prioritize” appears fourteen times. The strategy stipulates that CISA will “*prioritize* our actions to achieve the greatest impact…focus[ing] on four broad sets of stakeholders: (1) federal civilian executive branch agencies…(2) target rich, resource-poor entities where federal assistance and support is most needed…(3) organizations that are uniquely critical to providing or sustaining National Critical Functions…and (4) technology and cybersecurity companies with capability and visibility to drive security at scale.” This is a great start, but in tying the framework back to objective 2.1 of the CISA strategy, “understand how attacks really occur – and how to stop them,” [11] for OT/ICS, it is clear that many stakeholders that exist within and between the levels of the iceberg model are missing.

Another example of a disconnect between the strategy and reality of OT, the CISA enabling measure to “develop a robust capacity to analyze information about cybersecurity intrusions and adversary adaptation, and derive insights into which security measures were, or could have been, most effective in limiting impact and harm”[12] will not provide holistic awareness of the most consequential scenarios to prioritize for asset owners. For reasons previously outlined, this enabling measure in OT and ICS may highlight a gap or limitation in one aspect of OT and ICS cybersecurity for a particular stakeholder, but applicability will vary.

[7] JD Work (@HostileSpectrum), “Every time one sees an official advocating for a ransomware payment ban, the correct response is not to debate the policy failure modes that result from such…” Twitter, March 11, 2024, https://x.com/HostileSpectrum/status/1767172187176182031.

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

[9] “National Cybersecurity Strategy,” Office of the National Cyber Director, March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[10] “CISA Cybersecurity Strategic Plan FY 2024-2026,” Cybersecurity and Infrastructure Security Agency, August 4, 2023, https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf.

[11] “CISA Cybersecurity Strategic Plan FY 2024-2026.”

[12] “CISA Cybersecurity Strategic Plan FY 2024-2026.”

With continued emphasis on collaboration, on March 7, 2024, the Government Accountability Office (GAO) added to CISA's functional requirements four recommendations approved by the US Department of Homeland Security (DHS) to improve CISA's OT products, services, and collaboration. Specifically, the GAO report recommended that CISA:

1. measure customer service for its OT products and services;
2. perform effective workforce planning for OT staff;
3. issue guidance to the sector risk management agencies on how to update their plans for coordinating on critical infrastructure issues; and
4. develop a policy on agreements with sector risk management agencies with respect to collaboration. [13]

The first recommendation requires outreach and an audit of asset owners to understand the accessibility and usefulness of CISA products, services, and collaboration. It realistically requires a parallel review of the challenges that in-house security teams are tackling and the security controls and processes that are outsourced to the private sector. The second recommendation addresses a major need across the entire federal government and cybersecurity market. The third is currently the responsibility of each of the Sector Risk Management Agencies (SRMAs), including but not limited to CISA, which "coordinate and collaborate with DHS and other relevant Federal departments and agencies, with critical infrastructure owners and operators, [and] where appropriate with independent regulatory agencies and with state, local, tribal, and territorial (SLTT) entities."[14] Finally, the fourth recommendation has essentially been replaced by the directives of National Security Memorandum 22 (NSM-22), published on May 3, 2024. NSM-22 directs the Secretary of Homeland Security, acting through the Director of CISA, to "coordinate with SRMAs to fulfill their roles and responsibilities to implement national priorities consistent with strategic guidance and the National [Infrastructure Risk Management] Plan and continuously strengthen a unified approach to critical infrastructure security and resilience."[15] A more robust consideration from the GAO review might include CISA hiring and developing internal sector-specific subject matter experts to act as attachés for additional SRMAs. Many sector experts do exist at specific agencies, but very few specialize in cybersecurity, particularly for OT and ICS.

In February 2024 the President's Council of Advisors on Science and Technology (PCAST) released a report on cyber-physical resilience. Recommendations included:

1. establish sector-specific performance goals;
2. bolster and coordinate research and development;
3. break down silos and strengthening government cyber-physical resilience capacity; and
4. develop greater industry, board, CEO, and executive accountability.[16]

The report also calls on the federal government to "clarify the what and why of the national critical functions list to help each sector prioritize,"[17] which the GAO previously recommended in GAO-22-104279 published in March 2022.[18] The report also suggested the creation of a National Critical Infrastructure Observatory.

In March 2024, a draft report from the President's National Security Telecommunications Advisory Committee (NSTAC) suggested that economic incentives, liability tied to risk mitigation, and regulatory simplification tied to the National Institute for Standards and Technology's Cyber Security Framework (which CISA's Cybersecurity Performance Goals do quite well) provide a path toward strengthening national security and emergency preparedness.[19] The NSTAC also suggested the establishment of a Cybersecurity Measurement Center of Excellence to coordinate the management and assessment of existing data sources across the federal government.

These lists of competing priorities suggest many good ideas but often lack measurable milestones and deliverables. Critical infra-

[13] "Improvements Needed in Addressing Risks to Operational Technology," Government Accountability Office, March 7, 2024, https://www.gao.gov/assets/d24106576.pdf.

[14] "Sector Risk Management Agencies," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies.

[15] "National Security Memorandum on Critical Infrastructure Security and Resilience," The White House, April 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

[16] "Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World," The White House - President's Council of Advisors on Science and Technology, February 2024, https://www.whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.

[17] "Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World."

[18] "Critical Infrastructure Protection," Government Accountability Office, March 1, 2022, https://www.gao.gov/products/gao-22-104279#summary_recommend.

[19] "Measuring and Incentivizing the Adoption off Cybersecurity Best Practices," President's National Security Telecommunications Advisory Committee, March 2024, https://www.cisa.gov/sites/default/files/2024-02/2024.02.12_DRAFT_NSTACM%26IReport_508c.pdf.

structure stakeholders cannot address these challenges without an overwhelming amount of support and coordination. Recent initiatives express a vast amount of support for critical infrastructure but demonstrate a lack of coordination in addressing technical and procedural considerations for OT and ICS among relevant stakeholders. These competing priorities are also now being compared against more mandatory requirements like incident reporting and potential future sector-specific mandatory requirements.

For example, on March 27, 2024, CISA released the proposed rules issued to implement cyber incident reporting under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), passed in 2022. This comes just two months after updates to the Security and Exchange Commission (SEC) Rule 17 went into effect, covering Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. The SEC rule requires public companies to annually disclose material information about their cybersecurity risk management, strategy, and governance, and to disclose a significant cyber incident within four days of defining it as significant.

Covered entities under the proposed CIRCIA legislation would be required to report a "substantial cyber incident" within seventy-two hours. The rule applies "to entities in critical infrastructure sectors that either exceed the small business size standard (as set by the Small Business Administration) or meets any sector-based criterion."[20] CISA anticipated the criteria would impact over 316,000 businesses and organizations in the United States.[21] As legal scholars dig into increasingly mandatory policy measures like CIRCIA, they are uncovering new challenges for several regulated entities.

Cybersecurity attorney Megan Brown noted that the use of existing disparate and diverse best practices and frameworks "can be harmful if the regulator takes an idea or concept created for one use and imports into a different context for which it is ill-suited or – worse – fails to consider the similarities and differences. Use of unclear or shifting definitions and approaches can be unfair to regulated entities who lack predictability."[22] CIRCIA rulemaking "does not explicitly differentiate incidents based on what type of system or data was targeted or where the system is geographically located."[23] Taken into consideration with all the other goals and requirements, incident reporting is largely perceived as a burden not shared by the wider OT ecosystem but instead placed on asset owners and operators.

This regulatory landscape creates a challenge: how can stakeholders work together to prioritize actions, activities, and cost-benefit analysis if the federal government continues to present a sea of frameworks, best practices, suggestions, and voluntary and mandatory regulations? Without a harmonizing source of guidance across agencies, authorities, and well-intentioned bodies, there are few trusted advisors for stakeholders pursuing actions and activities. Each organization must choose which ideas and mandates to follow, defining their own champions and priorities, reviewing and mapping their operations risks based on the available standards, regulations, suggestions, and best practices.

RECOMMENDATIONS

Whoever is tasked with holistic harmonization among these various groups and agencies, there needs to be more robust synchronization beyond creating partnerships, points of contact, and building trust. Many of the needs and recommendations from available reports and strategies exist in current projects and resources that require stitching together across various federal projects and public-private partnerships. The following recommendations are intended to streamline previous suggestions and existing resources across the federal government, targeting the event, pattern, structure, and mental models of OT and ICS.

It is essential to establish which entities will be responsible for reviewing what is already available to avoid recreating many existing projects and data sources. Barring the creation of yet another organization or agency, these recommendations assume CISA has the homeland security mandate–authority derived from the National Cybersecurity Strategy and NSM-22 and directed tasks from the GAO–to facilitate the following recommendations:

1. streamline available OT and ICS cybersecurity data
2. align public-private risk researchers and analysts
3. conduct Cybersecurity Performance Goal (CPG) reviews with low, mid, and high-maturity organizations
4. expand training and awareness

[20] Rajesh De et al., "Proposed Rule Issued to Implement Cyber Incident Reporting for Critical Infrastructure Act," Mayer Brown, March 29, 2024, https://www.mayerbrown.com/en/insights/publications/2024/03/proposed-rule-issued-to-implement-cyber-incident-reporting-for-critical-infrastructure-act.

[21] Rajesh De et al., "Proposed Rule Issued to Implement Cyber Incident Reporting for Critical Infrastructure Act."

[22] Megan L. Brown, "As Cyber Regulators Rush Toward New Rules, Shifting Foundations May Complicate Compliance," Wiley, April 1, 2024, https://www.wileyconnect.com/As-Cyber-Regulators-Rush-Toward-New-Rules-Shifting-Foundations-May-Complicate-Compliance.

[23] Rajesh De et al., "Proposed Rule Issued to Implement Cyber Incident Reporting for Critical Infrastructure Act."

STREAMLINE AVAILABLE OT CYBERSECURITY DATA

As the NSTAC report suggested, data is a central missing factor for OT cybersecurity. The PCAST report suggested the United States should map its infrastructure to outmatch adversaries in discovering and addressing vulnerabilities and concentration risk. Building a national asset inventory depending on the install base could lead to a better understanding of the penetration rate of various vendor products, but doing so will not illuminate their networked implementations, configuration settings, or compensating controls introduced by asset owners and end users. CISA and existing SRMAs should consider streamlining available industry projects, resources, and data.

For example:

- CISA has a program coordinating executive authorities to subpoena telecommunications companies for network information with manufacturers to identify internet connected assets and drive down risk exposure.

- The MITRE Corporation recently unveiled the EMB3D Framework, which gives device makers a common understanding of vulnerabilities in their technologies, as well as the security mechanisms for addressing those weaknesses.[24]

- Since 2020, the OT cybersecurity industry has maintained the Programmable Logic Controllers (PLC) Security Top 20 List and interactive dashboard to improve the security posture of industrial control systems. These practices leverage natively available functionality in PLCs and Distributed Control Systems (DCS).[25]

Data from these programs can inform stakeholders from all levels of the iceberg model, producing shared priorities and outcomes for owners, operators, and product manufacturers. This improved coordination would produce a shared understanding of connectivity and targeting and hardening techniques.

The PCAST report also recommended the creation of a National Critical Infrastructure Observatory, to "develop a single national system that can support the overlay of key elements like active incidents, indications and warnings and act as a national virtual fusion environment for coordination."[26] Streamlining available data would allow the National Critical Infrastructure Observatory as a central body to not only identify deployed systems and determine their sector and use case, but also owners' and operators' risk posture, security concerns, tolerance for downtime, and prioritization efforts for defense and resilience.

Other examples of complementary programs and pilots without centralized data and gap analysis include programs such as:

- **CISA's Cyber Sentry** is "a CISA-managed threat detection and monitoring capability, governed by an agreement between CISA and voluntarily participating critical infrastructure partners who operate significant systems supporting National Critical Functions."[27]

- **The Department of Energy's CyTRICS** program works with industry partyers "to identify high priority OT components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing."[28]

- **The Electricity ISAC Cybersecurity Risk Information Sharing Program** shares data collected "through information sharing devices (ISDs) installed on participants' networks. Data collected through CRISP is used to identify cyber threat actors, pinpoint emerging trends, and analyze correlations across the sector."[29]

- **Idaho National Labs' Malcolm** is an open-source network traffic analysis tool designed to make network traffic analysis accessible to both the public and private sectors, supporting all sixteen critical infrastructure sectors.[30]

This type of monitoring and trends analysis is essential for stakeholders at the pattern and structure levels and can inform and incentivize ways to expand and replicate industry initiatives that create specific and actionable best practices. It is nonsensical to focus separately and simultaneously on bolstering asset owner security posture, analyzing external risks, measuring security controls, and mapping relevant government standards and compliance regimes. Lastly, this data can inform interdependence research that will be critical for government funding and policy prioritization moving forward.

Researchers in Canada recently published a time-series analysis of sector interdependency. Using twenty-five years of industrial

[24] "MITRE, Red Balloon Security, and Narf Announce EMB3D – A Threat Model for Critical Infrastructure Embedded Devices," MITRE, December 13, 2023, https://www.mitre.org/news-insights/news-release/mitre-red-balloon-security-and-narf-announce-emb3d.

[25] "Top 20 Secure PLC Coding Practices," PLC Security Top 20 List, https://plc-security.com/.

[26] "Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World," President's Council of Advisors on Science and Technology.

[27] "CyberSentry Program," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/resources-tools/programs/cybersentry-program.

[28] "CyTRICS," Idaho National Laboratory, US Department of Energy, https://cytrics.inl.gov/.

[29] "Cybersecurity Risk Information Sharing Program," Electricity Information Sharing and Analysis Center, https://www.eisac.com/s/crisp.

[30] "Malcolm," Idaho National Laboratory, US Department of Energy, https://inl.gov/national-security/ics-malcolm/.

statistics from 1997-200, they compare Gross Domestic Product (GDP) to the production of finished goods and services per sector, and the transactional use of goods and services by each to create finished products. Their findings generate two indicators: "weak correlations which likely indicate interdependency risks," and "strongly correlated but imbalanced interdependencies, which often indicate unmanaged supply-chain vulnerabilities."[31] CISA, in partnership with other agencies, should conduct similar research to capture interdependence correlations among and between sectors on a national level.

ALIGN PUBLIC-PRIVATE RISK RESEARCHERS AND ANALYSTS

Though most attacks on OT, ICS, or cyber-physical processes bear some similarities, each is unique, frustrating automated response and remediation as complete solutions.[32] Signatures, tactics, techniques, and procedures vary widely. This is further complicated by the fact that, in some cases, many owners and operators believe the risk of altering control systems outweighs the benefits of security controls. Unfortunately, this creates a situation where every organization must independently prioritize product vulnerabilities, researcher details, and disclosures. This is a major roadblock for efficacy, situational awareness, and strategic planning across the SRMA communities.

In many cases, organizations can only learn shared signatures, detections, and intelligence after another organization is victimized. Today, no single stakeholder could corroborate threat research information from two different publicly available OT or ICS cybersecurity resources. Where one publishes more details about indicators of compromise or tactics, techniques, and procedures witnessed in one sector, it may be because it has more customers in that sector and is not necessarily indicative of the threat landscape there. No method for standardizing, correlating, and collating threat and vulnerability research from market leaders exists currently.[33]

There are also several novel academic findings that detail existing vulnerabilities and capabilities the private sector has been working on for at least a decade. While the government does not typically provide a list of products to reverse engineer, security research teams often lack centralized insights to inform their own prioritization of research. The ICS Joint Cyber Defense Collaborative (JCDC) within CISA can facilitate enhanced mission alignment for the community by spearheading the development of a technical working group to align researchers and analysts in their approach to security research for industrial control systems, embedded devices, and OT in a more coordinated fashion.

Connecting these research dots would be significantly impactful for CISA's strategic objectives, helping to understand where attacks really occur and how to stop them. Therefore, the ICS JCDC should also establish a team and goal to create a better sense of the OT and ICS threat landscape beyond researchers. This would require working together with stakeholders from the data sources listed as part of recommendation one and harnessing available threat information from proprietary OT network monitoring solutions. These improvements, as well as championing ways to produce earlier warnings for exploitation and compromise indicators, would establish more proactive defense mechanisms before adversaries can build exploits.

CONDUCT CYBER PERFORMANCE GOALS REVIEWS WITH LOW, MID, AND HIGH RESOURCED ORGANIZATIONS

The CISA Cyber Performance Goals (CPGs) are general controls and security practices serving as a living document, with checklists enabling asset owners and end users in critical infrastructure to evaluate their systems' progress and maturity.

CISA should convene an independent OT Cybersecurity Advisory Board of voluntary, unbiased individuals, without a financial stake in OEM or cybersecurity products and separate from the SRMAs. To meet with the advisory board for private guidance, asset owners must review their CPG maturity and self-attest their level of CPG implementation by scope, cost, impact, and complexity. The ICS and Cybersecurity Divisions at CISA and the relevant JCDC leaders should work together to sort and review asset owners based on their maturity levels to discuss OT and ICS workflows, data streams, products, services, and recommendations coming from CISA and intended for these entities.

This volunteer board would meet with each maturity level group per quarter to review their progress and pain points with the CPGs. In the first quarter the board would meet with less well-resourced organizations with little to no implementation; second quarter meetings would focus on mid-level organizations with several controls and practices; and in the third quarter the board would meet with high-level maturity organizations with many cybersecurity partners and solutions working together to achieve most or all of the CPGs. In the fourth quarter, the independent advisory board, JCDC teams, and representatives from each

[31] Tyson Macaulay, "Critical Infrastructure Interdependency: Measuring a Moving Target," *Pulse & Praxis: A Journal for Critical Infrastructure Protection, Security and Resilience*, March 4, 2024, https://doi.org/10.5683/SP3/Y2CMPZ.

[32] Danielle Jablanski, quoted in William Loomis, "Modernizing critical infrastructure protection policy: Seven perspectives on rewriting PPD21," Atlantic Council, March 22, 2023, https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/modernizing-critical-infrastructure-protection-policy-seven-perspectives-on-rewriting-ppd21/.

[33] Danielle Jablanski, quoted in William Loomis, "Modernizing critical infrastructure protection policy: Seven perspectives on rewriting PPD21."

Sector Coordinating Council would convene to discuss lessons and challenges to reflect in CISA offerings.

Periodic maturity reviews of CPG implementation can provide necessary baselines and, in turn, inform the analysis questions raised above, without proposing sector-specific additions. This review also organically unpacks the many tolerance considerations of each asset owner and their risk posture. These baselines, together with the new and available data sources outlined previously, will address prioritization objectives–like identifying top federal resource allocation needs, which systems really need to get off the internet, addressing legacy system vulnerabilities, product logic and configuration best practices, change management, and more robust training and awareness programs.

EXPAND TRAINING AND AWARENESS

CISA is the *de facto* hub for critical infrastructure cybersecurity knowledge and shares resources with many partners. As the agency continues to review the use of its resources by partners and the public, a concerted effort is needed to resurrect relevant documentation and workstreams to promote learning and understanding for OT and ICS cybersecurity. Working with groups like the International Society of Automation, the OT Cybersecurity Coalition, and others can facilitate broader and more strategic reconceptualization of risks and priorities across OT and ICS, focusing primarily on awareness and advocacy.

Just like existing industry programs, pilots, and data sources, several worthwhile training programs exist that can be strengthened and offered to larger audiences to educate, train, exercise, learn, understand, and build resilience. For example, the CISA ICS Training in the Virtual Learning Portal and in person with the Idaho National Lab can be expanded and promoted to many more organizations that may not have internal OT expertise.[34] The International Society of Automation's microlearning modules, including basics like "Cybersecurity for CISOs" and similar modules can be promoted and required training.[35]

Many industries have their own resources and groups for training and education, including the information sharing and analysis center (ISAC) communities, exercises like GridEx, Radics, and Liberty Eclipse for the electric sector, industry associations like the National Rural Electric Cooperative Association (NRECA) and American Public Power Association (APPA), research arms like the Cybersecurity Manufacturing Innovation Institute (CyManII), and so on. What is clearly missing is a centralized understanding and cohesion of these similar efforts which can sometimes be perceived by stakeholders as noncomprehensive or feudal, depending on their financial and membership models.

Expansion and shared outcomes from these and similar exercises can form the foundations for behavioral changes that target the attitudes, beliefs, expectations, and values of the OT and ICS industries. In the future, a significant behavioral norm equivalent to "patch Tuesday" activities in IT security may emerge, becoming second nature for owners and operators. For example, more concerted efforts for "islanding" operations or disconnecting sites from more integrated and digitized SCADA systems could become more commonplace, where owners and operators are more equipped to safely and securely practice failure modes and manual operations.

Finally, every emergency begins and ends somewhere local. Emergency planning for asset owners should be a mandated requirement by SRMAs. For example, the Incident Command System for Industrial Control Systems (ICS4ICS) is designed to improve global ICS cybersecurity incident management capabilities and planning. ICS4ICS leverages the Incident Command System, as outlined by FEMA, for response structure, roles, and interoperability. The Incident Command System has been tested for more than thirty years of emergency and non-emergency applications, throughout all levels of government and within the private sector.

CONCLUSION

In 2019, the Federal Cybersecurity Research and Development Strategic Plan noted that as cyber-physical systems "become more complex, the interdependence of components increases the vulnerability to attacks and cascading failures."[36] Despite this realization, policy ideas, implementation, and standards continue to focus on vulnerabilities and attacks, with less attention paid to the systemic approaches. Between 2020 and 2024, the number of OT and ICS cybersecurity incidents exceeded the total number reported between 1991 and 2000.[37] Despite this increase in targeting, risks to OT and ICS have not changed drastically since a 2003 GAO hearing on "Critical Infrastructure Protection: Challenges in Security Control Systems."[38]

[34] "ICS Training Available Through CISA," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/ics-training-available-through-cisa.

[35] "Microlearning Modules: A New Learning Tool for Automation Professionals Involved in Cybersecurity," International Society of Automation, https://www.isa.org/training/microlearning-modules.

[36] "Federal Cybersecurity Research and Development Strategic Plan," National Science and Technology Council, December 2019, https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf.

[37] Mark Cristiano, "Cyber Regulation Roadmap: Navigating OT Security," *Industry Today*, January 23, 2024, https://industrytoday.com/cyber-regulation-roadmap-navigating-ot-security/.

[38] Danielle Jablanski, "Show Don't Tell: Four Ways to Address Cyber Risks to Energy Systems," Guidehouse, May 17, 2021, https://energycentral.com/o/Guidehouse/show-don%E2%80%99t-tell-four-ways-address-cyber-risks-energy-systems.

Each critical infrastructure entity is a vessel delivering products, resources, or services–with a complex system of interdependent digitized systems. Largely non-federal organizations, these entities require consistent and centralized strategy, leadership, and funding. Not incorporating all stakeholders in the relevant policymaking processes results in overlapping and incongruent policy, a range of voluntary and mandatory standards and best practices, and an overall reactionary stance in a discipline and domain that consistently benefits from ample planning and preparedness.

More clearly defined, coordinated, and shared objectives must be applied across all layers of the iceberg model. This level of coordination will begin to answer the many open questions related to the lack of available data and also help install base awareness of OT and ICS vendor technologies, the threat landscape, and the unique potential for cascading impacts each asset owner faces. Prioritization and understanding vendors, owners and operators, and national security and defense policymakers require a reconceptualization around priorities for OT cybersecurity–its events, patterns, structures, and mental models.

A key component of this reconceptualization will be the understanding of overlapping cyber risks, operational redundancy, and tolerance. These principles, best understood by each and every asset owner with cyber-physical infrastructure, produce the contingency planning and muscle memory required for resilience. The stitching together of numerous current activities, projects, technologies, and data sources will also require more personnel to contend with the complexity of this problem set and the evolving risk and threat landscape.

ACKNOWLEDGMENTS

The author thanks the following peers for contributing feedback on earlier versions of this paper and ideas and discussion during its creation: Blake Benson, Mark Bristow, Alphaeus Hanson, Trey Herr, Katherine Hutton, Karrie Jefferson, Will Loomis, Rob Morgus, Jen Pedersen, Sean Plankey, Sarah Powazek, Austin Reid, Matt Rogers, Megan Samford, Stewart Scott, and Joe Slowik.

ABOUT THE AUTHOR

Danielle Jablanski is an ICS cybersecurity strategist at the U.S. Cybersecurity and Information Security Agency (CISA), serving in the Office of the Technical Director. As the lead for ICS strategy, she is responsible for expanding the utility and reach of ICS products and services, coordinating internal and external stakeholder efforts, and maximizing public-private efforts for the OT and ICS cybersecurity industry and critical infrastructure owners and operators. She is also a nonresident fellow at the Cyber Statecraft Initiative of the Atlantic Council's Scowcroft Center for Strategy and Security. As time allows, Jablanski is also an advisor at Kutoa Technologies, and an Adjunct Professor teaching Intro to ICS Cybersecurity at Dallas College. Jablanski has been responsible for conducting academic and market research on emerging technologies throughout her career. She has independently consulted for the US government and a technology startup on novel technology applications for the military, Department of Defense, and commercial sectors. She began her career with the Stanley Center for Peace and Security evaluating cyber technology impacts to nuclear weapons policy and use worldwide. Before returning to the world of physical and industrial cybersecurity, Jablanski was a senior research analyst with Guidehouse Insights and spent the two years prior contributing to the creation and development of the Stanford Cyber Policy Center at Stanford University.

Disclaimer

Danielle Jablanski previously worked as an OT Cybersecurity Strategist in the private sector. The information, arguments, and recommendations presented in this issue brief were written and provided prior to her joining the Cybersecurity and Infrastructure Security Agency full time in May 2024.

Atlantic Council

Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org