HOW TO OUTPACE CYBER THREATS TO CRITICAL INFRASTRUCTURE

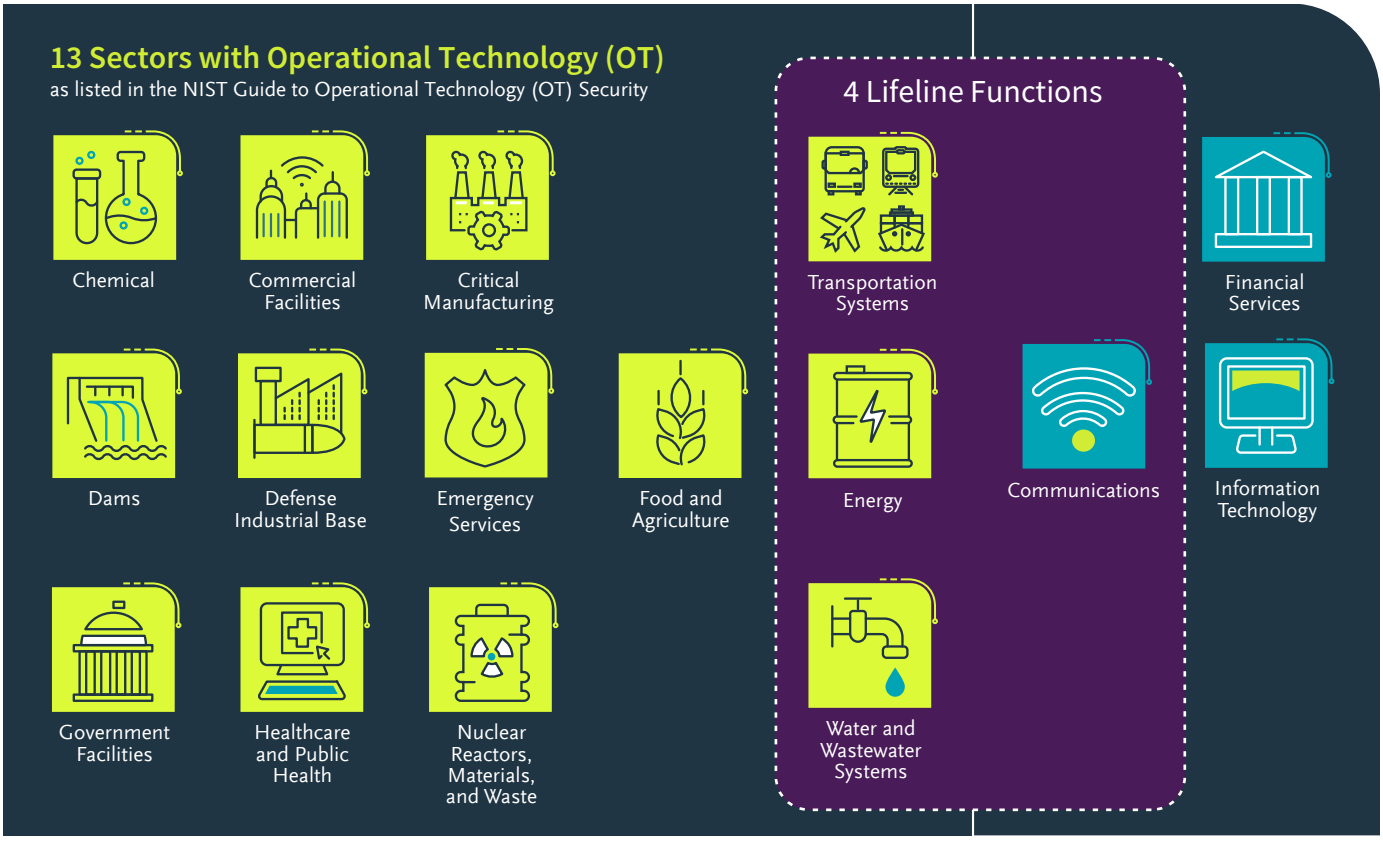
An OT/ICS guide to uncovering and managing systemic risk

Cybersecurity for critical infrastructure has reached a turning point. It's clearer than ever that today's cyber threats drive tomorrow's national security risks. Adversaries surreptitiously target the software, hardware, and services that vital industries rely on. They're seeking ways to sabotage lifeline functions like energy and water to achieve geopolitical and military objectives. The cybersecurity decisions that government and business leaders make today, or put off, could one day be decisive in conflict, crises, or competition. This is why the Joint Cyber Defense Collaborative (JCDC) 2023 Planning Agenda sets specific priorities for reducing systemic risk.

These **priorities** include securing operational technology and industrial control systems (OT/ICS), mainly from open-source software (OSS) risks; advancing cybersecurity and supply chain risk management, particularly for small- and medium-sized businesses; deepening operational collaboration in the energy sector; and protecting edge devices in the water sector. The overall aim is to reduce the spread of risk across interdependent systems so a failure of one area doesn't cause system-wide consequences. For critical infrastructure businesses, however, these priorities are about both risk and reward: They add up to an emerging opportunity to better sustain operations with grace under pressure and advance strategic business objectives.

The world runs on OT/ICS. These systems are largely owned and operated by the private sector. They support day-to-day operations for many control system processes like oil and gas exploration, production, distribution, and refining; electric power generation, transmission, and distribution; and water, wastewater, and public utilities. They're particularly crucial in "lifeline functions"—the four designated sectors where disruption or loss would trigger severe cascading effects on other sectors—but they're also used in many other industries. By strengthening the security and resilience of these systems against emerging cyber risks, businesses can advance national security and their own efforts to thrive and stand out in the marketplace.

THE 16 CRITICAL INFRASTRUCTURE SECTORS



Most business and cyber leaders aren't confident their organization is cyber resilient, according to the World Economic Forum's **research**: Many say their organization needs strong growth and improvement in cyber resilience despite following common practices, while others either have concerns or believe their organization isn't cyber resilient. Also, more than half say the third-party entities they depend on in their supply chain are less cyber resilient than their own organization. Moreover, most of the leaders surveyed doubt their board of directors can uphold a duty of care when it comes to cybersecurity. But now organizations can use JCDC's priorities to inform internal deliberations about emerging cyber risks in the C-suite and the boardroom and foster more confident management of these challenges with security and resilience.

No single report could ever address all facets of the challenges in the JCDC Planning Agenda, and that is not our goal here. Instead, this guide is intended to help critical infrastructure owners and operators accelerate efforts to uncover and manage systemic risk on the path to a more secure and prosperous tomorrow. It aims to complement cyber defense planning by providing context on trends, insights, on leading practices, and actionable advice on building security and resilience. It may also help inform internal discussions with leadership about cybersecurity investment plans. In addition, we've included practical steps that government and industry leaders can take to advance critical infrastructure cybersecurity by harnessing the power of artificial intelligence (AI).

KEY TRENDS

Cyberattacks on critical infrastructure are now top of mind around the world: They rank among the top five risks in the World Economic Forum's 2023 list of global risk perceptions. Also, cyberattacks on the United States rank among Americans' greatest concerns in the 2023 Munich Security Index global survey findings.

In our view, several longstanding trends, and a few newer ones, have shaped the current state of affairs.

Trends in Cybersecurity for Critical Infrastructure

- The IT/OT convergence of cyber and physical systems has outpaced cyber risk management.
- Legacy systems and OSS programs aren't designed to meet today's cybersecurity standards.
- Supply chains—for software and beyond—are vast, growing, opaque, and being subverted.
- Attack surfaces keep expanding: IoT (many kinds), 5G, cloud, OT/ICS, and remote work.
- Organizations are drowning in security data—not maximizing its potential.
- Trust gaps pose persistent obstacles for collaboration.
- Regulation is likely to increase and be consistent with the National Cybersecurity Strategy.
- Determined hackers keep innovating (e.g., tactics, techniques, procedures, and technology).
- Emergent malicious tools are designed to exploit OT/ICS vulnerabilities at scale.

OT/ICS THREATS: A CLOSER LOOK

Common types of ICS include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). Executives know these systems need protection, but gaining visibility and securing diverse OT/ICS networks is very challenging. Meanwhile, threat actors can easily access devices and designs, exploit vulnerable IT elements, abuse external connections and remote-access capabilities that have expanded attack surfaces, and employ increasingly dangerous hacking tools.

Now, threats are intensifying. The U.S. intelligence community's **latest annual worldwide threat assessment** is "particularly focused on improving its ability to target critical infrastructure," including undersea cables and ICS, and the People's Republic of China (PRC) is "almost certainly ... capable" of launching cyberattacks that could disrupt U.S. critical infrastructure, "including oil and gas pipelines, and rail systems."

Here is a look at how threat actors typically plan and carry out compromises against critical infrastructure control systems based on a five-step framework **articulated** by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA):

1. The adversary establishes the intended effect and picks a target. These plans will vary by the actor. While nation-states seek geopolitical advantages, ransomware groups recognize that OT networks are among the most valuable assets owned by critical infrastructure businesses, so they target these networks to spark quick ransom payments.
2. The adversary collects intelligence about the target system by conducting open-source research, using insider threats, or hacking enterprise networks. Forget the old cybersecurity adage about "security through obscurity." Hackers might find OT devices using Shodan, Censys, or other obtainable scanners. Metasploit is now integrated into Shodan and contains several OT exploit modules ready for use. Also, hacker forums share videos, tools, and tradecraft so novices can learn attack methods.
3. The adversary prepares to compromise the target by first developing and practicing techniques and tools that can be used to navigate and manipulate the system once initial access is gained. The tools may be readily available or custom built.
4. The adversary gains initial access to the system, often by abusing remote access capabilities designed to give vendors, integrators, service providers, owners, and operators access to the system.
5. The adversary executes techniques and tools to create the intended effect, such as disrupting, disabling, denying, deceiving, and/or destroying the system.

A key concern is the recent discovery of malware designed to exploit OT/ICS vulnerabilities at scale. Traditionally, OT exploits were bespoke and heavily tailored to the target environment (e.g., Stuxnet). But the IT/OT convergence has led developers of discrete products to reuse code and functionality—including OSS—inadvertently creating widespread shared vulnerabilities and risks in the marketplace. In 2022, it was revealed that advanced persistent threat (APT) actors had created a malware toolkit known as Pipedream (or Incontroller) that is capable of endangering countless OT/ICS targets with an array of automated malicious actions.

Pipedream exploits a reliance on common industrial network protocols (including some open-source protocols) in ICS vendor software supply chains. By using standard protocol functions, the toolkit acts like a "legitimate client or a development environment for programming the controller," according to a Codesys security advisory. Once an adversary gains initial access, the tools can be used to scan, compromise, and control targeted OT devices. These tools "have a modular architecture and enable cyber actors to conduct highly automated exploits against targeted devices," the U.S. government **warned**. Given that the malware is based on software widely used in PLCs, it is **reportedly** adaptable to "work in almost any industrial environment." Moreover, Pipedream was **reportedly** part of a Russia-linked operation targeting U.S. electric and gas facilities. Without commenting on reports about the operation, a senior Department of Energy official **said** Pipedream "was, in many ways, a fundamental shift in the cyber capabilities that are out there." The official cited the toolkit's ability to "take advantage of normal processes in systems across the board to potentially cause destructive effects."

There have been other software supply chain risks to OT/ICS security. The widely publicized Log4Shell vulnerability in the Java-based logging package Log4j, which came to light in 2021, affected a wide range of IT and OT systems. Log4Shell isn't primarily known as an OT vulnerability, but it's embedded in countless commercial software products that use open-source code. This shows how OSS ICS vulnerabilities can be tied to broader issues affecting all kinds of systems. Other examples of software-related ICS security challenges include code dependencies revealed in recent years: Urgent11, Ripple20, Amnesia33, and BadAlloc.

Examples of Software Supply Chain Risks Affecting OT/ICS

Urgent11	Ripple20	Amnesia33	BadAlloc	Log4Shell	Pipedream
2019: Major OT vendors relying on real-time operating systems (RTOS) are affected by network protocol vulnerabilities in the Interpeak IPnet TCP/IP* stack. Exploitation could allow remote code execution.	2020: Many ICS devices are affected by vulnerabilities in the Treck TCP/IP* stack. Exploitation may allow remote code execution or exposure of sensitive information.	2020: Many connected devices are affected by vulnerabilities embedded in open-source TCP/IP* stacks. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.	2021: Memory allocation vulnerabilities in multiple RTOS and supporting libraries could be exploited to create unexpected outcomes like a crash or a remote code injection/execution.	2021: An OSS vulnerability affects consumer and enterprise services, websites, applications, and OT products. An unauthenticated remote actor could exploit the vulnerability to take control of an affected system.	2022: An APT malware toolkit exhibits the capability to gain full system access to multiple ICS/supervisory control and data acquisition (SCADA) devices by exploiting common protocols, including open-source protocols.

* *Transmission Control Protocol/Internet Protocol*

Source: CISA advisories

Ultimately, no one organization or sector can manage such risks alone. For instance, industries such as electricity and natural gas need to increase cross-sector coordination on supply chain risk management related to commonly used hardware and software inputs, according to the National Infrastructure Advisory Council of industry and government executives. More cross-sector analysis is needed to better understand how simultaneous equipment failures across multiple modes or sectors sparked by a common cause could trigger unanticipated widespread consequences, the panel concludes in a **recent study**.

UNCOVERING AND MANAGING SYSTEMIC RISK

So how can critical infrastructure organizations uncover and manage systemic risk issues captured in JCDC's Planning Agenda? The following table lists ideas for consideration. It is important to note that different organizations will have varying risk management maturity levels in different areas. When in doubt, performing an initial assessment can help an organization gauge maturity in a particular area, and plan targeted improvements.

Challenge	Uncover	Manage
Detect and address today's ICS threats	Traditional cyber protection mechanisms aren't always feasible for ICS. Gaining visibility into these environments to support cybersecurity is critical. But few OT environments have any advanced cybersecurity monitoring in place. It's essential to understand the **common challenges** in ICS threat detection: • Legacy equipment and vendor restriction limit endpoint tool coverage. • Sensitivity in ICS environments requires many tools to be passive. • No one tool/sensor can provide visibility into all threats. • Limited cybersecurity skills in operations and plant operations knowledge in the security operations center (SOC). • Threats are constantly changing, and adversaries are advancing techniques. OT monitoring requires a holistic solution. **Guidance** from the NSA and CISA can help organizations understand tactics, techniques, and procedures (TTP) that threat actors use to compromise **OT/ICS** assets, as well as recommended mitigations.	Identifying which parts of the organization have critical data and assets and prioritizing their security is essential. Build a robust capability that enables threat detection within the ICS environment using a combination of passive and active monitoring tools. Also, build out playbooks, processes and training needed to enable collaborative response efforts. Conduct regular ICS-focused tabletop exercises to practice these playbooks and hone skills. A four-step approach to building an ICS threat detection and response program involves creating a strategy, expanding visibility in the networks (including gaining an understanding of what normal looks like in your environment), enabling continuous detection and response functions, and facilitating effective response operations. A well-thought-out strategy contains an initial list of targeted use cases, a rollout plan containing a proof-of-concept phase, skill sets needed to perform the work, staff required to enable the work, and a basic timeline. Leverage CISA's **Guide to Securing Remote Access Software**, as well as lessons from the **Cyber Storm national exercise**. Also, select entities may be eligible for **CyberSentry**, a voluntary CISA-managed threat detection and monitoring capability for critical infrastructure IT/OT networks.
Explore opportunities to adopt zero trust	If an attacker can reach an OT/ICS system, the defender has in a sense already lost, which underscores the importance of network segmentation, isolation, threat detection, and **a zero trust cybersecurity mindset**. Embracing zero trust is about stepping up and owning the risk that threats can emerge inside, not just outside, traditional network boundaries—and it's about proactively countering these risks. There are three principles of zero trust: assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors. Cybersecurity teams can't just buy a zero trust architecture (ZTA) from a vendor. Instead, teams must scrutinize an organization's strengths and challenges with intention, and then chart a path to a ZTA while committing to a longer journey.	The **seven zero trust pillars** are aligned with the Department of Defense (DOD) zero trust **reference architecture** and CISA's **maturity model**: • User • Device • Applications and Workloads • Network/Environment • Data • Visibility and Analytics • Automation and Orchestration Using the pillars and governance combined with a zero trust maturity assessment model, you can rate the maturity of current capabilities in all seven zero trust dimensions. Applying zero trust to OT environments is an area of increasing interest, as this **recent article** from Idaho National Laboratory shows.

Challenge	Uncover	Manage
Improve supply chain risk management	Know your supply chain. Establish and maintain full awareness of the suppliers—including third, fourth, and fifth parties—who participate in the design, development, implementation, maintenance, and disposal of all products and services. Also, explore using the **MITRE System of Trust Framework**, which seeks to define, align, and address the specific concerns and risks that prevent organizations from trusting suppliers, supplies, and service providers. Manufacturers and suppliers of software used by critical infrastructure IT and OT/ICS should consider producing a software bill of materials (SBOM).	Apply new supply chain knowledge to inform more effective risk management. Prioritize risks. Conduct multifaceted, ongoing monitoring. Drive remediations quickly. Integrate these efforts into enterprise risk management. Leverage **guidance** from CISA. Apply the **SBOM** concept to reduce software supply chain risks. SBOMs will be crucial for providing organizations with the greater visibility they seek and enabling threat hunting. Also, support the spread of cybersecurity supply chain risk management (**C- SCRM**) practices via the related NIST National Cybersecurity Center of Excellence (NCCoE) **project**.
Proactively counter software supply chain threats	Consider using the **Trident Framework**, which depicts the sort of cross-functional effort needed to counter software supply chain threats. It shows how enterprises can build a unified defensive effort involving cybersecurity experts, acquisition professionals, and the chief information security officer. The first step for an organization aiming to create this digital trident is to implement an SBOM framework that meets the National Telecommunications and Information Administration's minimum elements.	Apply the **framework's five-step process** to proactively hunt for software supply chain threats. Along the way, threat hunters should glean lessons from use cases. Also, they should study, contribute to, and build data sets around software supply chain attacks. **Put lessons and insights into action** by developing informed hypotheses to start the hunt.
Double down on cybersecurity fundamentals	The need to uncover cyber risks by strengthening cybersecurity fundamentals cannot be understated. A 2022 **assessment** based on a survey of 1,200 executives from a range of industries found that only a third of organizations were implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework at an advanced level (and only 4 in 10 organizations had built their cybersecurity program on zero trust principles). Moreover, the Government Accountability Office **reported** last year that only three of 16 sector risk management agencies had determined the extent of their sector's adoption of the NIST Framework. Review **CISA Risk and Vulnerability Assessments (RVA)** to learn more about common attack methods and security gaps.	Look for opportunities to use the **NIST Cybersecurity Framework** to its full potential while also adopting **CISA's cross-sector voluntary Cybersecurity Performance Goals (CPGs)**. These goals are grouped using the five functions of the NIST framework. Examples of goals include changing default passwords; implementing phishing-resistant multifactor authentication (MFA); separating user and privileged accounts; and creating, maintaining, and exercising cybersecurity incident response plans. You can also learn more about **ongoing efforts** to update the NIST Framework and provide input where appropriate. In addition, small- and medium-sized businesses can leverage **CISA** and **NIST** guidance.
Adopt data-driven cybersecurity	Today, many security teams can't make the most of their data and hence can't deliver value for the entire organization. Teams are forced to choose which data to collect when technology advancements and security budgets are out of sync. And that means **agencies** and critical infrastructure **entities** are losing ground to worsening digital threats—because they aren't using data as an asset.	Begin to unlock the potential of your security data, recognizing the potential to advance strategic objectives. Businesses that embrace data-driven cybersecurity can gain a competitive advantage. Conduct an analysis and make the data available to whoever needs to consume it. Data access should be controlled centrally. Start normalizing data to provide better visibility into the enterprise.

Challenge	Uncover	Manage
Boost security and resilience for edge devices	In the water sector, for example, improve asset management by ensuring: • The OT equipment and software inventory includes offsite and remote devices • The asset management plan includes devices and equipment from external vendors • PLCs and sensors receive security updates as needed • Automatic update installation is functioning where feasible • Inactive devices are removed from the network • The entire operational configuration is backed-up or archived	Leverage cybersecurity capabilities such as firewalls with intrusion detection, edge security, and virtual private networks. Follow the (NCCoE) **project** on how the water sector's adoption of automation, sensors, data collection, network devices, and analytic software may also expand cyber vulnerabilities and related risks: Watch for recommendations on asset management, data integrity, remote access, and network segmentation. For 5G-specific questions, see content on **establishing a secure and resilient ecosystem**, **enabling continuous monitoring**, and **zero trust**.
Apply AI to spot and address vulnerabilities	Both government and industry can find new opportunities to apply AI to critical infrastructure cybersecurity by revisiting the concepts associated with the Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge, which aimed to build automatic defenses. For instance, to improve vulnerability identification and characterization, the government should consider investing in AI systems designed to accurately predict the likelihood that a vulnerability will be exploited. Also, current DARPA efforts to identify, characterize, model, and measure exploitable vulnerabilities in widely used mobile devices could be a good template for future government efforts to address critical infrastructure cybersecurity gaps.	To support the development of effective defensive cyber and monitoring solutions, the nation should foster greater connections between the data science and AI community and stakeholders across the nation's critical infrastructure industries. This would raise awareness about key nuances inherent in attacks on specific sectors, enabling developers to create tailored solutions to meet specific mission needs. Also, organizations should aim to use AI to augment (rather than replace) existing cyber tooling. And to strengthen remediation, the government and industry could consider large-scale investments that build on DARPA Grand Challenge findings about options for including more computer autonomy in cyber defense. DARPA's recently announced **AI Cyber Challenge (AIxCC)** is a step in the right direction.
Anticipate future threats	Proactively research the threat landscape as it applies to your industry, organization, and environment. Close knowledge gaps about technology, vulnerabilities, and malicious activity with open-source intelligence, including reports tailored to meet your organization's needs. Track alerts from **CISA**, other authorities, and cyber information sharing and analysis centers (ISACs). Review insights on **China's cyberattack strategy** and the logic behind **Russian military cyber operations**.	Adopt an intelligence-driven, threat-informed approach to cyber risk management, including exercises with realistic red teaming that leverage catalogs of the latest known vulnerabilities affecting networks, hardware, and software. Organizations lacking access to a sophisticated red team may benefit from using micro emulation plans developed for defenders by **MITRE Engenuity**.
Expand operational collaboration	Set the stage to collaborate. The more you know about the threat landscape and vulnerabilities as they apply to your organization through proactive research and beyond, the better positioned you are for greater operational collaboration within a given industry and across sector boundaries.	Commit to building trust and sharing actionable intelligence and insights on cyber threats. Craft the architectures that will facilitate and simplify collaboration: Beyond culture changes, technical architectures are key because if they're not in place, their absence becomes an obstacle to collaboration. In addition, leverage recent **National Infrastructure Advisory Council (NIAC)** recommendations for boosting cross-sector collaboration.

NEXT STEPS

Here are steps leaders can take now to help critical infrastructure organizations outpace cyber threats:

1. To advance ICS threat detection and response, create a high-level strategy before any people, process, or technology changes occur. A well-thought-out strategy contains an initial list of targeted use cases, a rollout plan containing a proof-of-concept phase, skill sets needed to perform the work, staff required to enable the work, and a basic timeline. Expand/maintain visibility into the environment. Baseline what "normal" looks like. Establish response rules of engagement and define what actions can be taken/escalated. Consider prepositioning incident response tools to expedite response and recovery.
2. Assess your organization's zero trust maturity. Also, watch for future federal guidance on applying zero trust in OT environments.
3. Assess your supply chain to truly understand it and its component parts, several layers down. Also, support emerging efforts to better understand and manage supply chain risk across sector boundaries.
4. Prioritize threat hunting for software supply chain threats.
5. Maximize the potential of the NIST Framework and CISA CPGs.
6. Assess opportunities to adopt a data-driven cybersecurity approach.
7. Leverage NCCoE insights to boost the security and resilience of edge devices.
8. Government leaders should consider funding and launching new initiatives that advance AI cybersecurity capabilities for critical infrastructure by building on the successes of past and current DARPA initiatives. Industry should prioritize participating in such initiatives while also making complementary investments.
9. Assess whether your organization fully leverages open-source intelligence (OSINT) research, collaboration, and anonymized cybersecurity data sharing to inform cyber risk management. Participate in sector-based information sharing and analysis centers (ISACs) to exchange data, insights, and leading practices about threats and mitigation strategies. Also, pursue opportunities to collaborate across sector boundaries.
10. Support better performance-based pressure testing in critical infrastructure sectors such as water and energy to help these sectors make needed investments in cybersecurity rather than postponing investments for fear of passing on costs to consumers. Conduct regular tabletop exercises to evaluate operational readiness and inform cybersecurity budget plans and decisions. Also, support the development of cross-sector cybersecurity drills.

EMPOWER PEOPLE TO CHANGE THE WORLD®

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining more than 100 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: Empower People to Change the World℠.