JULY 2020

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SECURING INDUSTRIAL CONTROL SYSTEMS:

A UNIFIED INITIATIVE

FY 2019–2023

Table of Contents:

Letter FROM THE Director

The Cybersecurity and Infrastructure Security Agency (CISA) is pleased to present Securing Industrial Control Systems: A Unified Initiative.

Through this "One CISA" initiative, CISA will work with critical infrastructure (CI) owners and operators to build industrial control systems (ICS) security capabilities that directly empower ICS stakeholders to secure their operations against ICS threats. We will also work to improve CISA's ability to anticipate, prioritize, and manage national-level ICS risk.

CISA is organizing its efforts around four guiding pillars:

- **PILLAR 1:** Ask more of the ICS community, and deliver more to them.
- **PILLAR 2:** Develop and utilize technology to mature collective ICS cyber defense.
- **PILLAR 3**: Build "deep data" capabilities to analyze and deliver information that the ICS community can use to disrupt the ICS Cyber Kill Chain.
- **PILLAR 4:** Enable informed and proactive security investments by understanding and anticipating ICS risk.

ICS security presents unique challenges. Traditional ICS devices used to manage industrial processes are difficult to secure without creating unacceptable disruptions to critical industrial processes. The large-scale use of newer technologies—such as 5G cellular networks, artificial intelligence, pervasive machine-to-machine communications, and advanced data analytics—introduces both advantages and additional uncertainties and may significantly change the ICS risk landscape.

Most importantly, because ICS manage physical operational processes, the increasing convergence of information technology (IT) and operational technology (OT) creates opportunities for exploitation that could result in catastrophic consequences, including loss of life, economic damage, and disruption of the National Critical Functions (NCFs)[1] upon which society relies.

Against this backdrop, the ICS community must aggressively pursue new ways to outpace our adversaries and elevate ICS security and resilience as a national priority. No entity has the resources or capabilities to counter all ICS threats alone. Rather, the future of ICS security lies in building collective ICS security capabilities through joint investments and collaboration with ICS cyber researchers as well as with our partners in government, the private sector, and academia.

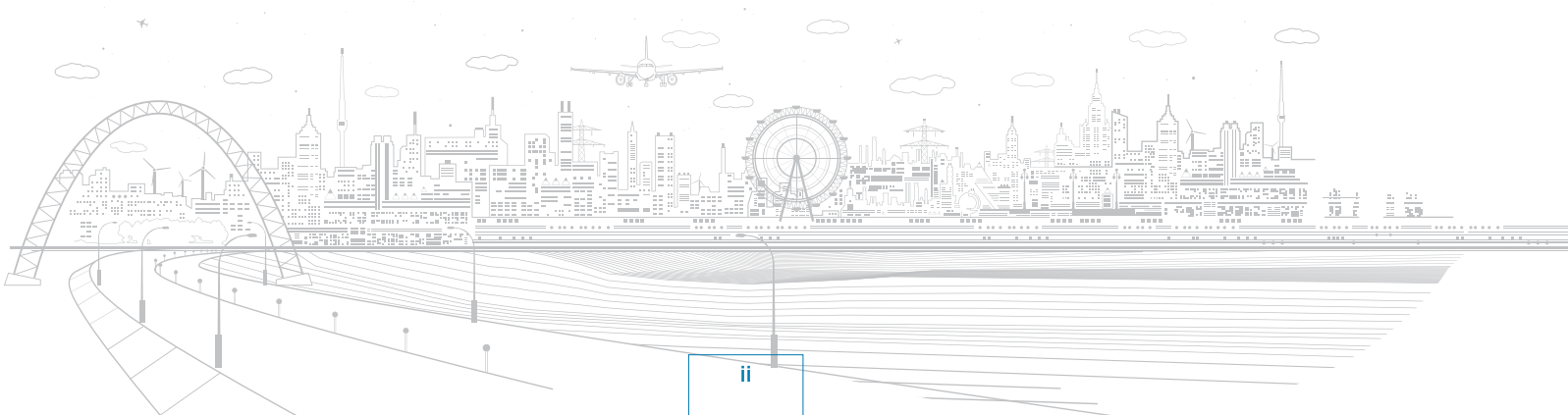
The work that CISA does will continue to support the ICS community. The analysis, training and exercises, vulnerability coordination, assessments, and response services we provide today will continue to make a real difference to the Nation's security. In addition, CISA's *Securing Industrial Control Systems: A Unified Initiative* will support national efforts to secure control systems in the areas of workforce development, standards and best practices, supply chain risk management, and incident management. We have made substantial progress since we first stood up an ICS security capability in 2004, but there is still more to do. Our adversaries are driven, imaginative, and persistent. Accordingly, we must be agile enough to counter them.

Through this initiative, CISA will build on the work we have already done—and continue to do—with the ICS community to create new ICS security capabilities that will markedly improve the way we defend ICS today and secure ICS for tomorrow.

Christopher Krebs,

Director, Cybersecurity and Infrastructure Security Agency

[1] https://www.cisa.gov/national-critical-functions-overview



INTRODUCTION

Securing Industrial Control Systems: A Unified Initiative lays out a five-year plan (Fiscal Years 2019—2023) that defines how CISA will prioritize and organize our approach to ICS security. This document contains the following sections:

SECTIONS 1 & 2: Introduction and CISA's ICS Vision	introduce the initiative, describe the end-state vision, and provide historical context.
SECTION 3: The ICS Challenge	describes the ICS risk environment in which CISA and the ICS community must operate to secure ICS.
SECTION 4: The Diverse ICS Community	emphasizes CISA's operational and strategic partnerships across the ICS community.
SECTION 5: Defending ICS Today	highlights portfolio of ICS capabilities CISA currently maintains and the products and services we deliver to the ICS community.
SECTION 6: Securing ICS for the Future	defines the four guiding pillars that focus this initiative.
SECTION 7: Conclusion	summarizes the initiative's primary drivers and focus.

This initiative aligns directly to the *National Cyber Strategy of the United States of America,*[2] *the Department of Homeland Security (DHS) Cybersecurity Strategy (FY 2019—2023)*,[3] and the operational priorities listed in CISA's 2019 *Strategic Intent*[4] document. The ICS initiative meets all ICS-specific requirements and directives contained in these overarching strategies.

[2] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[3] https://www.dhs.gov/publication/dhs-cybersecurity-strategy
[4] https://www.cisa.gov/sites/default/files/publications/cisa_strategic_intent_s508c.pdf

CISA'S ICS VISION

The security of ICS and other operational technologies is essential to achieving CISA's vision of **secure and resilient infrastructure for the American people**. Through implementation of this initiative, CISA and our partners will help the ICS community reach the following critical end-state conditions.

- **ICS performs within thresholds under duress.** ICS networks are resilient to cyberattacks and continue to perform within operational parameters in support of NCFs, despite malicious actions by adversaries in the control systems environment.
- **The ICS security community is faster and smarter than its adversaries.** Collaborating across industries and national borders, the ICS community raises the cost, time, and complexity thresholds for successful ICS attacks to the point that they exceed the capabilities of even the most advanced threat actors.
- **OT devices and networks are secure by design.** New OT products, from industrial scale control systems and networks to Internet of Things (IoT) devices, are secure by design. Cybersecurity becomes a preeminent consideration in the development and design of new OT products, and operators can apply security updates without operational disruption.
- **Risk drives ICS security priorities.** CI asset owners and operators distribute ICS security resources based on a clearly defined risk posture and risk tolerances, and the Federal Government invests resources based on ICS risks to the security and resilience of the NCFs.
- **Security resources are readily accessible to all.** Using broadly available and easily implemented ICS cybersecurity tools and services, CI asset owners radically increase their baseline ICS cybersecurity capabilities.

CISA pursues this vision by executing our mission to **partner with industry and government to understand and manage risk to our Nation's critical infrastructure.** CISA will work with our partners in the ICS community toward four enduring and cross-cutting pillars that together drive sustainable and measurable change to the Nation's ICS security risk posture:

1 PILLAR — **Ask more of the ICS community, and deliver more to them.**

2 PILLAR — **Develop and use technology to mature collective ICS cyber defense.**

3 PILLAR — **Build "deep data" capabilities to analyze and deliver information that the ICS community can use to disrupt the ICS Cyber Kill Chain.**

4 PILLAR — **Enable informed and proactive security investments by understanding and anticipating ICS risk.**

Each pillar drives CISA toward specific objectives that require incremental, evolutionary, or disruptive actions. Through implementation of each pillar's objectives, milestones, and activities contained in this initiative, CISA will:

- **Empower the ICS community to defend itself;**
- **Coordinate "whole community" response and mitigation capabilities to respond to the most significant ICS threats and incidents;**
- **Vastly improve the community's capability to ingest, synthesize, and provide actionable intelligence to ICS asset owners;**
- **Bring to bear the unified capabilities and resources of the Federal Government;**
- **Inform ICS investments and drive proactive risk management of National Critical Functions;**
- **Drive positive, sustainable, and measurable change to the ICS risk environment; and**
- **Move beyond reactive ICS defense to proactive ICS security.**

A PARADIGM SHIFT

This initiative places significant emphasis on developing joint ICS security capabilities—with partners in government and the private sector—that asset owners and operators implement directly to secure ICS. Through the deployment of these shared capabilities, asset owners and operators can better defend themselves while also helping to inform CISA's national-level ICS priorities. In addition to continuing to provide and improve our current ICS security products and services, CISA will prioritize development of ICS community-driven solutions.

NCFs are a critical focal point for CISA's ICS security strategy. CISA will highlight priority NCFs and map the architecture of these functions and identify the degree to which specific NCFs depend on ICS. CISA will also appropriately align our ICS resources to the areas where the destruction, disruption, or exploitation of ICS poses the greatest risk to NCFs.

The initiative also elevates ICS security as a priority within CISA, coalescing CISA's organizational attention around the implementation of a unified, "One CISA" strategy. Our OT cybersecurity experts, risk managers, CI and physical security experts, field operations, external affairs liaisons, strategists, stakeholder engagement liaisons, and technologists will collaborate on an ongoing basis to implement important aspects of this initiative.

NATIONAL CRITICAL FUNCTIONS

In 2019, CISA identified and validated a set of 55 National Critical Functions following extensive consultation with the CI community. These are, "the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." NCFs provide an important prism through which CISA can work with our partners to help them understand, prioritize, and address ICS risk.

Viewing these NCFs holistically provides a complement to CI sector-based approaches to risk management. CISA will gain greater clarity into the criticality of various elements of the Nation's infrastructure by focusing risk analysis on the specific ways that an entity supports NCFs. NCFs also help CISA understand dependencies and potential risks, including the impact that exploitation of ICS may have on the delivery of the essential products and services upon which the American people rely. By viewing risk through a functional lens, CISA can work with our partners to harden ICS systems across the CI ecosystem in a more targeted, prioritized, and strategic manner. A key forum for this work is the CISA-supported Critical Infrastructure Partnership Advisory Council (CIPAC), which enables the government and private sector entities—organized as coordinating councils—to engage in activities to support and collaborate on CI security and resilience efforts.

[5] https://www.cisa.gov/national-critical-functions-overview

[6] Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, establishes national policy on CI security and resilience. PPD-21 identifies 16 CI sectors and designates associated Federal Sector-Specific Agencies (SSAs) to lead Federal Government efforts to collaborate, coordinate, and implement actions to enhance the security and resilience of their respective CI sector. The USA Patriot Act defines CI as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (USA Patriot Act of 2001 (42 U.S.C. 5195c(e)).

THE ICS CHALLENGE

Much of the Nation's CI depends on ICS such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS), which rely on programmable logic controllers (PLC) to manage essential and complex operational processes.

Risk to traditional ICS once predominantly arose from human error and accidents, natural disasters, and acts of physical sabotage. Traditional ICS can have 30-year lifecycles and are purpose-built, stand-alone systems designed for reliability rather than security. The convergence of physical and cybersecurity processes and increasing integration of ICS with business networks and internet-based applications has vastly increased the prevalence and complexity of cyber threats to ICS. Unlike business enterprise networks, which manage information, ICS manage physical operational processes. Therefore, cyberattacks could result in significant physical consequences, including loss of life, property damage, and disruption of the essential services and critical functions upon which society relies. The use of cyberattacks to cause physical consequences make ICS attractive targets for malicious actors seeking to cause the United States harm.

Operational technologies are also increasingly commoditized, prevalent, and used in applications that may be smaller in scale than industrial processes, which further contributes to cybersecurity risk. These applications are growing exponentially and migrating into domains not previously automated or connected to the internet (e.g., automobiles, medical devices, smart buildings and homes, pipelines, aviation).[7] Adding to the ICS risk topography is the deployment of 5G networks, which reduces reliance on traditional network routers, thus limiting the ability of security providers to monitor for and prevent malicious traffic. CI owners and operators must navigate through this ICS risk landscape to deliver the essential products and services that support societal well-being and fuel the economy.

[7] More than 21 billion IoT devices are expected by 2025 (Source: The future of IoT: 10 predictions about the Internet of Things, https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html)

THE DIVERSE ICS COMMUNITY

CISA'S OPERATIONAL PARTNERSHIPS

At an operational level, CISA works with the following partners to enhance the community's ICS technical, analytical, and response capabilities: CI asset owners; ICS vendors and integrators; ICS-focused cybersecurity providers; researchers and academia; government at all levels; and international counterparts. CISA maintains operational relationships with numerous resident[8] and non-resident government and private sector organizations. Key operational partners include:

- DHS (including the Federal Emergency Management Agency, National Operations Center, Office of Intelligence and Analysis, the Science and Technology Directorate [including DHS Centers of Excellence], Transportation Security Administration, U.S. Coast Guard, and U.S. Secret Service);
- Department of Justice (Federal Bureau of Investigation [FBI]);
- Department of Defense (DOD) (U.S. Cyber Command and National Security Agency);
- Department of Energy (DOE) (including the National Laboratories);
- Federal Cybersecurity Centers;
  - FBI's National Cyber Investigative Joint Task Force
  - National Security Agency/Central Security Service Threat Operations Center
  - DOD's U.S. Cyber Command and Cyber Crime Center
- Intelligence Community Incident Response Center, Information Sharing and Analysis Centers (ISACs) (including the Aviation ISAC, Communications ISAC, Electricity Sector ISAC, Financial Services ISAC, Information Technology ISAC, and Multi-State ISAC), and Information Sharing and Analysis Organizations (ISAOs); and
- Individual CI owners and operators, including major telecommunications and internet service providers, ICS vendors and integrators, ICS cybersecurity providers, and other CI partners.

CISA'S STRATEGIC PARTNERSHIPS

In addition to those partners with whom CISA maintains ongoing operational relationships, CISA also manages longstanding strategic partnerships with organizations within the ICS community to support security and resilience activities across the risk management spectrum.

These vital strategic partnerships create trust within the ICS community, foster open communication, establish processes and procedures for action, and facilitate effective operational integration and coordination. The following are CISA's core strategic partners.

Control Systems Interagency Working Group (CSIWG): CSIWG is an interagency working group focused on defining a whole-of-community, strategic approach to control systems security. In coordination with the private sector, CSIWG is working to ensure U.S. Government priorities in the control system space meet the needs of the community. The working group serves as the strategic foundation for a unified effort to improve cybersecurity for control systems across the U.S. Government and private sector.

Industrial Control Systems Joint Working Group (ICSJWG): ICSJWG[9] represents a foundational public-private partnership through which CISA supports information exchange and development of risk management capabilities, products, and services. ICSJWG facilitates communication among federal, state, and local governments; asset owners and operators; vendors; system integrators; international partners; and academic professionals in all 16 CI sectors.

[8] "Resident" organizations have liaison officers that sit on CISA's Integrated Coordination and Operations Center watch floor.
[9] See https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

CISA plays a unique role as the lead federal civilian agency responsible for advising CI partners on how to manage ICS risk. Fulfilling this role successfully requires both operational and strategic partnerships across the ICS community. Such collaborative partnerships often succeed in resolving intractable issues where unilateral efforts of government or private industry cannot.

The diverse ICS community comprises entities with equities in ICS security, including federal, state, and local governments; asset owners and operators; vendors; system integrators; international partners; and academic professionals in all 16 CI sectors. This section highlights the major ICS community groups with whom CISA must collaborate to manage ICS risk successfully.

Federal Advisory Committees: On behalf of DHS, CISA is the designated federal agency responsible for supporting several federal advisory bodies that involve expertise in ICS and OT. These include numerous councils operating under CIPAC (which provides a mechanism for CI Sector and government coordinating councils, sector-specific agencies [SSAs], and working groups such as the Enduring Security Framework to collaborate on CI security issues), the National Security Telecommunications Advisory Committee (NSTAC), and the National Infrastructure Advisory Council (NIAC).

Other Non-Governmental Partners: CISA works extensively with ICS community leaders and influencers, the CI owners and operators that use and depend on ICS, ICS/OT vendors, researchers, security providers and consultants, ISACs and ISAOs, IT and cybersecurity professionals (chief information officers [CIOs], chief information security officers [CISOs], etc.), and non-governmental organizations such as academia and standards setting bodies. CISA leverages these partnerships to support unified strategic planning, technology development, preparedness planning and exercises, operational procedures and processes, training, research and development, security and threat awareness, development and promotion of ICS standards and best practices, information exchange, strategic risk and interdependency analyses, and numerous additional activities.

Congress and the White House: When called upon, CISA serves as a subject matter expert and advisor to Congress and the White House, helping to inform proposed cybersecurity laws and policy decisions.

Department of Homeland Security: CISA serves as the lead advisor to the Secretary of Homeland Security on CI and cybersecurity (including ICS security) matters. CISA also works closely with other DHS organizations to coordinate ICS security efforts and assist on specific ICS-focused initiatives.

Sector-Specific Agencies and other Federal Departments and Agencies: SSAs are federal departments and agencies that collaborate with government and the private sector to coordinate security initiatives for their designated CI sector. CISA works closely with SSAs that rely significantly on control systems for operation of CI, particularly in sectors that may have an elevated risk of cyberattack (e.g., Energy Sector, Critical Manufacturing Sector). CISA is also responsible for the security of the Federal Government's civilian networks and works with other federal agencies and several National Labs (under the umbrella of the Department of Energy) to help them protect against ICS threats as well as to coordinate ICS security efforts for their constituencies.

States and Localities: CISA partners with a range of state, local, tribal, and territorial (SLTT) governments, oversight and regulatory bodies, community leaders, law enforcement, homeland security advisors, state CIOs and CISOs, intelligence fusion centers, and emergency responders. CISA also coordinates with the Multi-State Information Sharing & Analysis Center (MS-ISAC), which supports cyber threat prevention, protection, response, and recovery for the Nation's SLTT governments.

International Partners: Cybersecurity is a global issue, and reducing cyber risk must involve a unified global effort. Cybersecurity incidents occurring in other countries—particularly those involving novel or persistent cyber threats—may have significant implications for ICS security in the United States. These and other considerations require strong international collaboration—including operational collaboration and integration—to support DHS's cybersecurity mission to protect our Nation's CI from cyber threats.

DEFENDING ICS TODAY

Every day, CISA works with CI asset owners and operators to help them identify, protect against, and detect cybersecurity threats and respond to and recover from significant incidents to both IT and OT networks (see **figure 1**).

Although ICS owners and operators manage their own security, when the potential exploitation of ICS technologies poses existential threats to people or property—or undermines confidence in CI safety and reliability and NCFs—it is CISA's mission to assist through delivery of a broad portfolio of ICS security products and services. CISA's current offerings include:

Figure 1

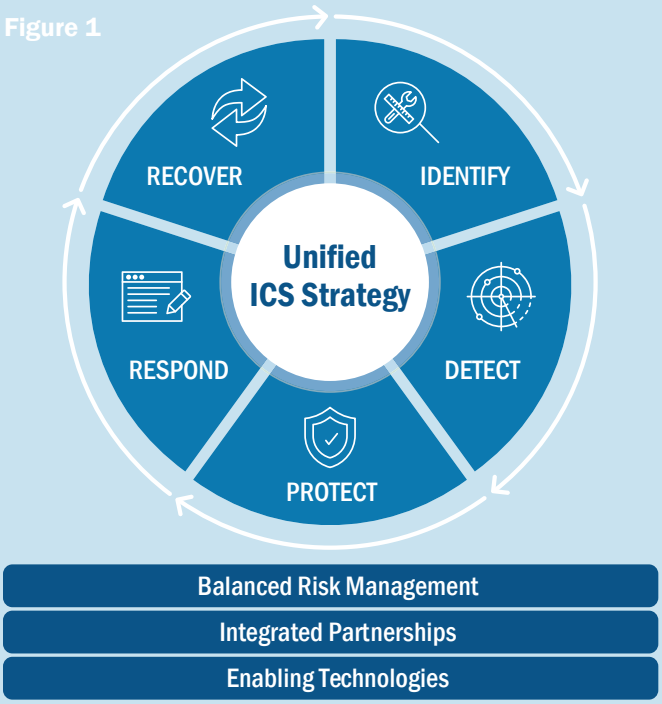


Figure 1: CISA provides full-spectrum ICS security capabilities to CI owners and operators.

Exercises and Training:

CISA supports continued improvement in cyber preparedness and resilience through ICS-focused cyber exercise design, development, and execution. CISA offers a range of exercise types, from tabletop discussions to full-scale, national-level exercises. ICS training capabilities include ICS security fundamentals as well as more advanced online and in-classroom training available for learners with a range of technical expertise. CISA also offers regional courses and workshops, as well as a recurring five-day, hands-on advanced training event.

Watch Operations:

CISA maintains an around-the-clock alerting and reporting function that helps maintain situational awareness across the ICS risk landscape. This includes receiving, monitoring, triaging, tracking, coordinating, and reporting on ICS cyber threats and events and, where possible, monitoring and tracking the tactics, techniques, and procedures (TTPs) of specific threat actors. The center also serves as the primary entry point for incoming reporting and service requests from CISA's partners as well as ICS task routing and dissemination within CISA.

Hunt and Incident Response:

- **Incident Response:** CISA serves as the Federal Government's primary mechanism for providing asset response capabilities to nationally significant cybersecurity incidents in U.S. CI, including ICS-specific incidents. CISA's goal is to assist victims, upon their request, to mitigate and minimize the duration and severity of ICS incidents. Incident response efforts focus on identifying the root cause of an incident by searching for adversary TTPs, behaviors, and associated artifacts in the victim network. CISA continues to expand our capacity for managing incident responses as well as our technical response tools and capabilities.

- **Hunt:** At the invitation of our partners, CISA also provides voluntary assistance to identify adversary presence in ICS environments via proactive hunt missions (conducted in the absence of a known incident). CISA's hunt capabilities are specifically focused on identifying sophisticated threats, often beyond the capacity and capability of traditional cyber security tools and techniques.

ICS Security Partnerships:

The operational and strategic partnerships CISA maintains with the global ICS community are the underpinning for enduring ICS security. ICSJWG is a critical foundational element to CISA's public-private partnerships. This working group supports information exchange and ICS risk-reduction strategies by fostering collaboration within industry and between industry and the Federal Government. CISA also hosts CSIWG, which works with interagency partners and the private sector to help drive the national strategic direction for control systems cybersecurity.

Strategic Risk Assessment:

At the strategic level, CISA's National Risk Management Center (NRMC) is a planning, analysis, and collaboration center focused on addressing the Nation's highest priority critical infrastructure risks, originating from cyberattacks and other hazards. NRMC serves as the end-to-end integrator of risk management activities for NCFs and leverages that risk expertise to support overall execution of the CISA mission. NRMC leads CISA efforts on supply chain risk management, engaging partners and performing analysis to identify and secure the supply chain of critical components. Further, NRMC provides CISA with expertise in methodology development, risk assessment, modeling, and data management and visualization.

OT Assessments:

CISA offers our partners a range of asset-based assessments, including Validated Architecture Design Reviews (VADR), which involve an architecture design review, system configuration and log review, and network traffic analysis. We also provide the Cybersecurity Evaluation Tool (CSET)—a downloadable self-assessment tool with an ICS focus—at no cost to customers. In addition, CISA's protective security advisors can conduct evaluations of physical security protections for ICS, including Regional Resiliency Assessment Program (RRAP) assessments, which help contextualize the role of ICS in enabling CI functions and provide information about the potential regional consequences of their disruption. Such assessments also consider the resilience of essential services (e.g., electric power, communications) that enable ICS to function. In turn, this information informs ICS preparedness and planning efforts regarding redundancies, service backup, and alternate operating modes. Lastly, CISA's chemical security inspectors conduct compliance assistance and regulatory inspections for certain ICS.

Information Exchange:

CISA shares the outputs of our analysis with the ICS community through a wide range of cybersecurity information products, including ICS-focused alerts, advisories, analysis reports, and best practices. CISA's information products provide either raw data—usually IOCs—or analysis products that help asset owners and operators prevent, detect, and mitigate threats and vulnerabilities.

Technical and Threat Analysis:

To understand and identify ICS threats, CISA conducts a wide range of analysis with the intelligence community, researchers, vendors, CI owners and operators, and other partners to develop, contextualize, and share indicators of compromise (IOCs). CISA also conducts analysis on malware, digital media, and ICS hardware. CISA ICS analysts focus on digital artifacts from devices specific to industrial control systems such as PLCs and remote terminal units. CISA's ICS advanced malware laboratory specializes in malware threats to ICS environments and provides asset owners with onsite or remote support.

Vulnerability Management:

CISA works with trusted partners in the public and private sector to coordinate timely and responsible disclosure of ICS cybersecurity vulnerabilities. CISA publicizes vulnerabilities and (when known) shares mitigation measures with users and administrators. CISA also works with ICS vendors and integrators to test new product lines to identify vulnerabilities before they go to market. CISA also works with our partners to understand hardware and software vulnerabilities in the ICS supply chain.

SECURING ICS FOR THE FUTURE

It is important that CISA continues to invest in and improve the capabilities, products, and services described in **Section 5**. However, when evaluating the Nation's emerging security challenges, CISA must—in partnership with the ICS community—move well beyond what we are doing today by building our ICS strategy around four cross-cutting pillars.

PILLAR ONE:

ASK MORE OF THE ICS COMMUNITY, AND DELIVER MORE TO THEM.

VISION: CISA will reinvigorate and deepen our existing partnerships while also expanding the scope of engagements with the broader ICS community to empower CISA's partners to mitigate ICS risk.

CISA'S FOCUS: No single entity can successfully manage the scope and complexity of the entire ICS risk landscape. The ICS community's path to security lies in a truly integrated government-industry alliance, founded on trust and transparency and focused on strategic and operational collaboration across the community. Such an alliance engages private sector CI owners and operators; ICS manufacturers, vendors, and integrators; researchers; cybersecurity firms; academia; international partners; government agencies; law makers and regulators; and other stakeholders in a global effort to understand and mitigate ICS risk. By combining its collective security resources and expertise, the ICS community can radically amplify ICS risk-management capabilities and shape joint security investments that shift the cybersecurity paradigm.

PILLAR TWO:

DEVELOP AND UTILIZE TECHNOLOGY TO MATURE COLLECTIVE ICS CYBER DEFENSE.

VISION: CISA will develop and promote easily accessible, deployable, and inexpensive ICS tools and capabilities to help asset owners secure ICS against all adversaries.

CISA'S FOCUS: Current ICS security technology focuses on reactive defense against known threats with limited capabilities to detect threats based on behavior rather than pre-defined indicators. CISA will work with the ICS community to drive technology developments that harden the cybersecurity defenses of legacy control systems, build security into new ICS devices while in the development stage, and increase lower-level data visibility. CISA will approach development of ICS cybersecurity technologies by leveraging the inventiveness and the wisdom of the ICS community to ensure CISA products do not inhibit ICS functionality. CISA will also make a broader range of CISA-developed capabilities readily available to CI asset owners and operators. In addition, CISA will incentivize partners to develop and implement ICS security technologies to protect themselves and their customers.

PILLAR THREE:

BUILD "DEEP DATA" CAPABILITIES TO ANALYZE AND DELIVER INFORMATION THE ICS COMMUNITY CAN USE TO DISRUPT THE ICS CYBER KILL CHAIN.

VISION: CISA will diversify data partnerships, further define ICS data needs, and support efforts to increase the ingestion of additional data differentiated by source, type, and consequence to increase visibility into ICS threats and vulnerabilities.

CISA'S FOCUS: With greater access to data and better quality and fidelity of data, CISA will vastly improve our analytic capabilities and can provide better threat and vulnerability information to our partners. As CISA matures our ICS vulnerability management program, we will map discovered vulnerabilities to product lines and configurations to understand with accuracy the vulnerability's impact and potential consequences. CISA will use the information we collect—not only to improve the depth and value of the threat and vulnerability data we provide partners—but also to develop configuration gold standards and to enable third parties to leverage CISA capabilities to perform hunt, malware analysis, and other ICS analytic functions.

PILLAR FOUR:

ENABLE INFORMED AND PROACTIVE SECURITY INVESTMENTS BY UNDERSTANDING AND ANTICIPATING ICS RISK.

VISION: CISA will improve visibility into the risk landscape and use that knowledge to inform investments into proactive initiatives that move the ICS community ahead of the threat curve.

CISA'S FOCUS: CISA will work to understand the severity of ICS cyber risks (including threats, vulnerabilities, and consequences) and the effect our actions—both those currently undertaken in defense of ICS and those implemented through this initiative—have on the ICS risk to NCFs. CISA will use the best information available to perform risk analysis that informs investments across the ICS stakeholder community. CISA will also gain better understanding of CI and NCF dependencies on ICS and use risk and consequence analysis models to understand the full impacts of ICS cyberattacks. Further, CISA will dedicate resources to future studies and trend analysis that help the ICS community understand impact of new innovations on ICS cybersecurity environments, anticipate emergent risk, drive preemptive action, and inform risk investment priorities. CISA will ensure that our understanding of strategic risks informs our priorities for assessments and that what is learned from assessments informs our understanding of strategic ICS risks.

CONCLUSION

As CISA implements this initiative over the next several years, the ICS threat environment will surely evolve. CISA will adapt to changes in the environment and manage specific ICS risk management activities accordingly; the foundational pillars around which this initiative builds will endure.

Sustainable success for ICS security requires CISA to understand the ICS community's priorities and work with them to close security gaps. To do this effectively, CISA will expand and deepen trusted partnerships across the ICS community so that more organizations and technical experts contribute the data, expertise, and ideas CISA requires to succeed in our mission. Similarly, CISA will work with ICS technology leaders to jointly develop, incentivize, and share innovative ICS cybersecurity technologies that lower implementation barriers for CI owners and operators. CISA will also enhance the quality and fidelity of the data we collect, which will enable us to provide high quality, action-focused analytical products that are tailored to the unique requirements of specific customers.

Most importantly, CISA and the ICS community must know the impact our actions have on the national ICS risk landscape, particularly with respect to NCFs. With this knowledge, together we will work as a single, unified organization that achieves sustainable and enduring ICS security and drives wise, risk-informed ICS security investments.