IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CISA INDUSTRIAL CONTROL SYSTEMS SECURITY OFFERINGS

DEFEND TODAY,
SECURE TOMORROW

CISA INDUSTRIAL CONTROL SYSTEMS SECURITY OFFERINGS AND CAPABILITIES

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating with industry to build more secure and resilient infrastructure for the future. CISA partners with the industrial control system (ICS) community to help understand, detect, and protect against ICS risk, and, when necessary, helps critical infrastructure (CI) owners and operators respond to significant cybersecurity incidents.

CISA’S ROLE IN ICS SECURITY

CISA plays a unique role as the lead federal civilian agency responsible for helping CI partners manage ICS risk. Fulfilling this role 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.

Broadly, the ICS community includes all entities—government at all levels, the private sector, international partners, academia, and others—with equities in ICS security. CISA’s focus on ICS security and commitment to collaborating with the ICS community is a vital part of its mission.

OFFERINGS

To support the ICS community's cyber risk management efforts, CISA offers a wide range of products, services, and capabilities. **Click on any icon below** to learn more.

See the Resources section at the end of this document to visit CISA webpages for each offering.

Assessments
Operational resilience evaluations

Cyber Hunt
Aid ICS partners with adversary presence search in absence of known threat

Exercises
Testing and readiness for ICS incidents

Information Exchange
Sharing of threat and best practice guidance with partners

Partnerships and Engagement
Collaborate and coordinate with ICS partners

Products and Tools
Access to hands-on tools for the ICS community

Response
Provide expertise and advanced tooling to aid ICS cyber victims

Strategic Risk Analysis
Provide ICS risk information pertaining to National Critical Functions (NCFs)

Technical Analysis
ICS malware analysis support

Training
Technical and non-technical ICS instruction for all skill levels

Vulnerability Coordination
Coordinated, public disclosure of ICS vulnerabilities + mitigation recommendations

ASSESSMENTS

CISA offers a range of voluntary cybersecurity assessment services focused on Operational Technologies (OT) that evaluate an organization's:

- Operational resilience
- Cybersecurity practices
- Management of external dependencies
- Additional elements that are key to a robust cybersecurity framework

Stakeholders receive recommendations and mitigation plans for all assessments. Information shared with CISA by the requestor is confidential and may be protected as Protected Critical Infrastructure Information (PCII) (https://www.cisa.gov/pcii-program).

Visit https://www.cisa.gov/cyber-resource-hub or call 888-282-0870 for more information on how to request assessment services.

CYBER HUNT

CISA's hunt capabilities are specifically focused on identifying sophisticated threats and adversary presence in OT and IT environments, often beyond the capacity and capability of traditional cybersecurity tools and techniques.

EXERCISES

CISA provides cyber exercise planning to support ICS and critical infrastructure partners by delivering a full spectrum of cyber exercise planning workshops and seminars. These range from small discussion-based exercises that last two hours to full-scale, internationally scoped, operations-based exercises that span multiple days. CISA designs these events to assist organizations at all levels in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities.

CISA designed the CISA Tabletop Exercise Package (CTEP) to assist partner organizations in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders. The CTEP allows users to leverage pre-built exercise templates and vetted scenarios to build tabletop exercises to assess, develop, and update information sharing processes, emergency plans, programs, policies, and procedures.

To request more information about the CISA exercise program, visit https://www.cisa.gov/critical-infrastructure-exercises or email Central@cisa.dhs.gov. Visit https://www.cisa.gov/publication/cisa-tabletop-exercise-package to access the CTEP document and guides.

INFORMATION EXCHANGE

CISA regularly publishes ICS-specific alerts, advisories, and guidance documents for the public. Alerts provide timely notification to critical infrastructure owners and operators concerning control systems threats. Advisories provide timely information about current security issues, vulnerabilities, and exploits.

To view CISA's latest alerts and advisories and ICS best practice guidance documents, visit https://www.cisa.gov/ics and click on resources tab.

Automated Indicator Sharing Program

CISA's free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).

AIS is a part of CISA's effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. AIS is free to all ICS partners. Want to learn more? Visit https://www.cisa.gov/automated-indicator-sharing-ais or call 888-282-0870.

PARTNERSHIPS AND ENGAGEMENT

The Industrial Control Systems Joint Working Group (ICSJWG) supports information sharing and reduced risk to the Nation's ICS through enhanced collaboration between the Federal Government and private owners and operators of ICS across all CI sectors. ICSJWG facilitates partnerships between Federal, state, and local governments; asset owners and operators; vendors; system integrators; international partners; and academic professionals in all 16 CI sectors. The ICSJWG encourages closer collaboration between government and industry through the ICSJWG Steering Team (IST).

ICSJWG activities and products include:

- In-person meetings
- Webinars
- Newsletters

ICSJWG membership is voluntary and free to all ICS stakeholders. Members receive all outgoing communication to the ICSJWG community, including newsletters (with content submitted by ICSJWG membership), face-to-face meeting invitations, announcements, training information, and calls for comments. For the latest ICSJWG event information, or to learn more about becoming an ICSJWG member, visit https://www.cisa.gov/icsjwg.

PRODUCTS AND TOOLS

CISA provides the ICS community the opportunity to access the following tools to help strengthen their cybersecurity posture.

- ***The Cyber Security Evaluation Tool (CSET®)*** provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate ICS and IT network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations. CSET is available as an open-source tool on GitHub: https://github.com/cisagov/cset/wiki.
- ***The Control Environment Laboratory Resource (CELR)*** is a test range environment for government and private industry partners to experience the possible effects of kinetic cyber physical attacks. CELR allows users to perform security research on ICS and supervisory control and data acquisition (SCADA) systems.
- ***CyberSentry*** is a voluntary pilot program that leverages best in breed, commercial off-the-shelf technologies, such as network intrusion detection tools, to identify malicious activity in CI ICS and corporate networks. CyberSentry participation increases real-time visibility into U.S. CI and provides the capability to detect nation-state adversaries on CI networks and derive cross-sector analytic insights.
- ***Malcolm*** is an open source, easily deployable network traffic analysis tool suite which enables the user to capture full network packet artifacts (PCAP files) and logs in OT/ICS environments. Malcom provides unique insight into specific protocols used in ICS environments. Because Malcom comprises only open-source tools, it does not require users to obtain paid licenses.

To request additional information on CELR, CyberSentry, or Malcom, call 888-282-0870 or email central@cisa.dhs.gov.

RESPONSE CAPABILITIES

When cyber events impact physical processes, CISA can help asset owners by coordinating risk mitigation efforts across the ICS community and sharing indicators of compromise and tactics to secure the Nation's infrastructure. CISA brings expertise and advanced tooling to aid ICS cyber victims in identifying artifacts, determining affected components, and building recovery plans specific to lower-level OT devices. To report an ICS incident, visit https://us-cert.cisa.gov/report or call 888-282-0870.

STRATEGIC RISK ANALYSIS

CISA provides ICS partners with resources and capabilities to manage ICS risk through CISA's National Risk Management Center (NRMC). NRMC is a planning, analysis, and collaboration center focused on addressing the Nation's highest priority CI risks—originating from cyber threats and physical hazards. The Center also focuses on integrating previously siloed risks. At the strategic level, NRMC serves as the end-to-end integrator of risk management activities for the National Critical Functions (NCFs) and leverages that risk expertise to support overall execution of the CISA mission.

To learn more about NRMC's key initiatives and to access resources, please visit https://www.cisa.gov/national-risk-management. To explore information about the NCFs, visit https://www.cisa.gov/national-critical-functions.

TECHNICAL ANALYSIS

CISA has the ability to conduct 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 is able to provide owners with support. To report malware, please visit https://us-cert.cisa.gov/report.

TRAINING

CISA's ICS training courses and workshops provide the ICS community no-cost, in-person and virtual training. Visit https://www.cisa.gov/cybersecurity-training-exercises to explore training options.

Topics covered include:

- Introduction to ICS security
- Defense strategies
- Information on cyber threats
- How to coordinate response with DHS
- Mitigations for vulnerabilities

VULNERABILITY COORDINATION

CISA's Coordinated Vulnerability Disclosure (CVD) program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). This includes new vulnerabilities in ICS, Internet of Things (IoT), medical devices, as well as traditional IT vulnerabilities.

The goal of the CVD program is to ensure CISA, the affected vendor(s) and/or service provider(s), and the vulnerability reporter all disclose simultaneously. This ensures users and administrators receive clear, consistent, and actionable information in a timely manner.

To report an ICS vulnerability, call 888-282-0870, or visit https://us-cert.cisa.gov/report.

RESOURCES

Offering/Capability	Website
Assessments	• https://www.cisa.gov/cyber-resource-hub • PCII Program: https://www.cisa.gov/pcii-program
Exercises	• https://www.cisa.gov/critical-infrastructure-exercises • CTEP documents: https://www.cisa.gov/publication/cisa-tabletop-exercise-package
Information Exchange	• https://www.cisa.gov/ics > click on resources tab • AIS Program: https://www.cisa.gov/automated-indicator-sharing-ais
Partnerships and Engagement	• https://www.cisa.gov/ics > click on resources tab • https://www.cisa.gov/icsjwg
Products and Tools	• CSET tool: https://github.com/cisagov/cset/wiki • Email central@cisa.gov for other products and tools
Response Capabilities	• To report an ICS incident, visit https://us-cert.cisa.gov/report
Strategic Risk Analysis	• NRMC link: https://www.cisa.gov/national-risk-management • National Critical Functions (NCF): https://www.cisa.gov/national-critical-functions
Technical Analysis	• To report malware, visit https://us-cert.cisa.gov/report
Training	• https://www.cisa.gov/cybersecurity-training-exercises
Vulnerability Coordination	• https://www.cisa.gov/coordinated-vulnerability-disclosure-process • To report an ICS vulnerability, call 888-282-0870, or visit https://us-cert.cisa.gov/report