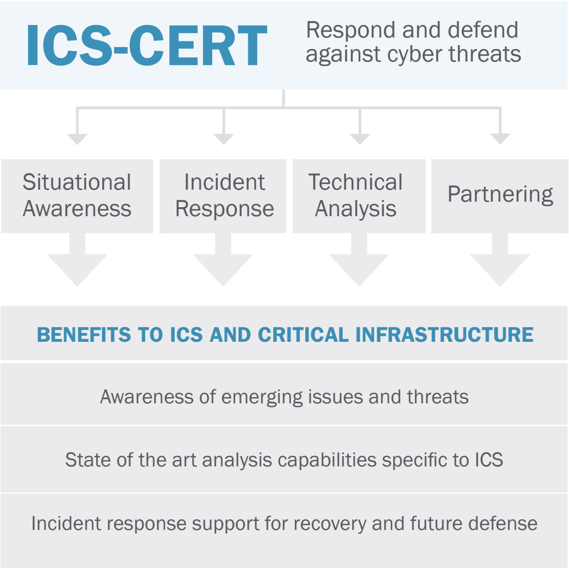
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is the operational arm of the Control Systems Security Program (CSSP). The U.S. Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) created both ICS-CERT and CSSP to combat rising cyber threats to critical infrastructure. ICS-CERT provides industrial control systems (ICS) stakeholders with incident response services, vulnerability coordination, situational awareness, and analytical support to effectively manage cyber threats and reduce risks.



ICS-CERT Respond and defend against cyber threats

Situational Awareness

Incident Response

Technical Analysis

Partnering

BENEFITS TO ICS AND CRITICAL INFRASTRUCTURE

Awareness of emerging issues and threats

State of the art analysis capabilities specific to ICS

Incident response support for recovery and future defense

PROTECTING AMERICA'S CONTROL SYSTEMS

ICS-CERT's mission is to reduce risk to critical infrastructure industrial control systems by providing incident response and tactical mitigation information to protect against emerging cyber threats. ICS-CERT accomplishes this by engaging with both private and public partners to share and fuse information in order to comprehensively assess the threat landscape and provide mitigations to the community at large. ICS-CERT leads this effort by:

- Responding to and analyzing control systems related incidents;
- Conducting vulnerability, malware, and digital media analysis;
- Providing onsite incident response services;
- Providing situational awareness in the form of actionable intelligence;
- Coordinating the responsible disclosure of vulnerabilities and associated mitigations; and
- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

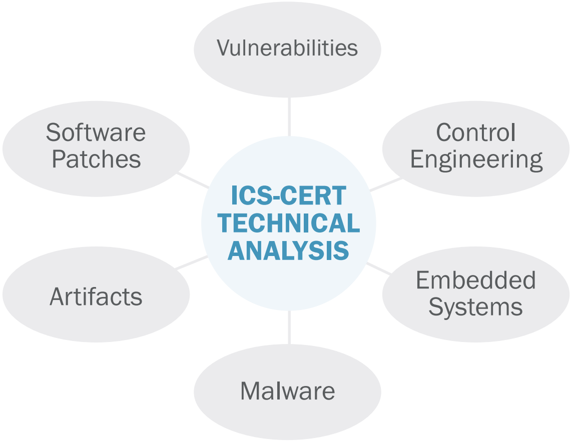
ICS-CERT is a key component of DHS's Strategy for Securing Control Systems. The primary goal of the Strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts.

Homeland Security

UNIQUE CAPABILITIES

ICS-CERT operates an Advanced Analytics Lab (AAL) to analyze vulnerabilities, perform digital media and log file analysis, and analyze malware threats to control systems environments. The AAL provides unique capabilities and technical expertise in both industrial control systems and cybersecurity. These capabilities include the ability to configure representative test environments of control system equipment commonly used within critical infrastructure to support this testing and analysis capability.

ICS-CERT leverages these capabilities to provide analytic services to companies requesting support in response to an incident. ICS-CERT is able to analyze hard drives, log files, malware, and other artifacts and provide detailed indicators and analysis reports to assist organizations in detecting and mitigating malicious activity.



PARTNERSHIPS

ICS-CERT works to reduce risks within and across all critical infrastructure sectors. In particular, ICS-CERT partners with law enforcement agencies and the intelligence community, coordinates efforts among federal, state, local, and tribal governments, and works with control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector CERTs to share control systems related security incidents and mitigation measures.

ICS-CERT also operates side-by-side within the National Cybersecurity and Communications Integration Center (NCCIC) with a variety of partners such as the United States Computer Emergency Readiness Team (US-CERT), to provide a single source of support to respond to cyber threats against industrial control systems.

ICS-CERT participates with many working groups including the Industrial Control Systems Joint Working Group and the Cross-Sector Cyber Security Working Group. These trusted relationships are leveraged to increase and improve information sharing with critical infrastructure and key resource asset owners and operators as well as the vendor community.

RESOURCES FOR ASSET OWNERS

ICS-CERT posts recommended practices guidelines, whitepapers, and alerts and advisories about ICS threats and vulnerabilities to the web at **www.ics-cert.org** and shares more sensitive information through the US-CERT secure portal. Asset owners can request access to the Control Systems Center compartment of the US-CERT portal by emailing **ics-cert@dhs.gov.**

REPORTING CYBER INCIDENTS AND EVENTS

CSSP and ICS-CERT encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Reports can be submitted to ICS-CERT via one of the following methods:

ICS-CERT Watch Floor: 1-877-776-7585

ICS Related Cyber Activity: ics-cert@dhs.gov

For general program questions or comments contact cssp@dhs.gov **or visit** www.us-cert.gov/control_systems.

ABOUT DHS AND NCSD

DHS is responsible for safeguarding our nation's critical infrastructure from physical and cyber threats that can affect our National security, public safety, and economic prosperity. The National Cyber Security Division (NCSD) is DHS' lead agency for securing cyberspace and our Nation's cyber infrastructure. ICS-CERT is operated by the CSSP under NCSD.

For more information visit www.dhs.gov/cyber.

Control Systems Security Program

PREPARING FOR CYBER INCIDENT ANALYSIS

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides guidance to critical infrastructure asset owners to assist in preparing their networks to handle and analyze a cyber incident.

Even the best cyber defense mechanisms cannot prevent all cyber incidents. The sheer volume of intrusions attempted against information technology systems every day creates the possibility that a cyber attack could penetrate the numerous defensive systems in place on many networks. In order to provide the swiftest incident response and recovery possible, preparation and planning are essential.

ESTABLISH SYSTEMS ANALYSIS CAPABILITY

The ability to identify the source of an incident and analyze the extent of the compromise is necessary to rapidly detect issues, minimize loss, mitigate exploited vulnerabilities, and restore computing services. Two comprehensive resources for developing an incident response capability are:

Developing an Industrial Control Systems Cybersecurity Incident Response Capability, 2009
www.us-cert.gov/control_systems/csdocuments.html

Computer Security Incident Handling Guide, 2008
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

OPERATIONAL PREPARATION

Cyber incidents are tense, complicated, and not often part of routine operations. When properly maintained, operational preparedness measures can ensure the availability of information necessary to recover from an incident quickly while minimizing the impact.

A dedicated incident handling team should be led by a senior technical staff member who has the authority to make key decisions in a timely manner. In addition to the lead and forensics analysts, the team should have stakeholders from the following groups: Corporate IT (both network and host management), Control Systems Subject Matter Experts, Public Relations, Legal Counsel, Law Enforcement (if necessary).

The team should be trained in proper incident handling techniques and should practice using the tools to establish and maintain proficiency. Operating procedures should be developed to include:

- Identification of objectives and goals of response
- Internal and external communications policy
- Meeting and briefing schedules
- Reporting to all required regulatory agencies

An overall incident preparedness checklist should be created and reviewed regularly. Documentation should be accessible to operations personnel to help facilitate analysis of the incident and indentify priorities for recovery. At a minimum, documentation should include:

- An up-to-date network map to include IP ranges, hostnames and roles for servers, ingress and egress points between sub-networks, and wireless access points and modems;
- Software and operating system names, versions, and patch levels;
- Account roles and policies;
- Firewall and IPS rule sets; and
- Contact lists and escalation points for Internet Service Providers (ISPs), Computer Emergency Response Teams (CERTs), and service, software and hardware providers.

Homeland Security

An incident response information gathering checklist should also be created. This checklist should identify the types of information that should be collected to aid analysis by external CERTs or partners. Examples of critical information may include:

- Affected IPs
- Method of detection
- Type of activity that occurred
- Whether activity is continuing
- Timeline information
- Evidence of compromise
- Type of assistance needed
- Potential operational impact
- Impact to control systems
- Points of contact

It is important to establish an "out-of-band" communications policy. Any communications regarding an incident or potential incident should not go through the standard communication channels, e.g. corporate email, VoIP systems, as these may already be compromised and will tip off the adversary that you are aware of their presence in your network. In addition, any files relating to the incident or your handling policy should be stored off of the network or at the very least protected using strong encryption and proper key management.

IMPORTANCE OF LOGGING

System and network device logs are essential to incident investigators. The types of logging that should be considered include Firewall, Proxy, DNS, DHCP, web app, A/V, IDS/IPS and host and application logs. Additional logging to be considered is flow data from routers, switches, and packet captures.

During an incident investigation, network administrators should be able to identify which internal hosts have communicated with which IP addresses and what type of traffic was generated. DNS queries, proxy activity, and unusual network activity (such as port scanning) are also important data that may be required during an incident investigation. Packet captures may help identify any data that was exfiltrated. System auditing features, log retention durations, and time synchronization should be managed properly.

Log integrity is essential during an incident investigation; therefore, logs should be continuously stored on a separate system, frequently backed-up, and cryptographically hashed to allow detection of log alterations.

PRESERVING FORENSIC DATA

Other critical components of incident response are forensic data collection, analysis, and reporting. These elements are essential to preserving important evidence. To avoid the loss of essential forensic data:

- Keep detailed notes of what is observed, including dates/times, mitigation steps taken/not taken, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.
- When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.
- Capture forensic images of the system memory and hard drive prior to powering down the system.
- Avoid running any antivirus software "after the fact" as the AV scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines.
- Avoid making any changes to the operating system or hardware, including updates and patches, as they will overwrite important information about the suspected malware.

Organizations should consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts. Additionally, ICS-CERT subject matter experts are available to aid in incident response activities. Affected entities should not hesitate to contact ICS-CERT for assistance. Control system environments have special needs that should be evaluated when establishing a cyber forensic plan. The ICS-CERT recommends the following source on control system forensics:

Recommended Practice: Creating Cyber Forensics Plans for Control Systems, Department of Homeland Security, 2008
www.uscert.gov/control_systems/pdf/Forensics_RP.pdf

ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

**For more information,
visit www.us-cert.gov/control_systems.**

Control Systems Security Program

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

Critical Infrastructure and Key Resources (CIKR) support the essential functions and services that keep America operating. Some CIKR elements are so vital that an interruption in their services could have a debilitating impact on national security and economic well-being.

Although each critical infrastructure industry is vastly different, all have one thing in common--they depend on industrial control systems (ICS) to monitor, control, and safeguard their processes.

ICS, also known as Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), are essential to industry and government because they support the operation of our Nation's CIKR Sectors. As such, the Department of Homeland Security (DHS) recognizes that the protection and security of ICS is essential to the economy and security of our Nation.

BRIDGING THE COMMUNICATIONS GAP

Within the National Cyber Security Division (NCSD) of DHS, the Control Systems Security Program (CSSP) established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate knowledge sharing between the Federal government and private sector owners and operators in all CIKR sectors in an effort to reduce the risk of ICS cyber threats.

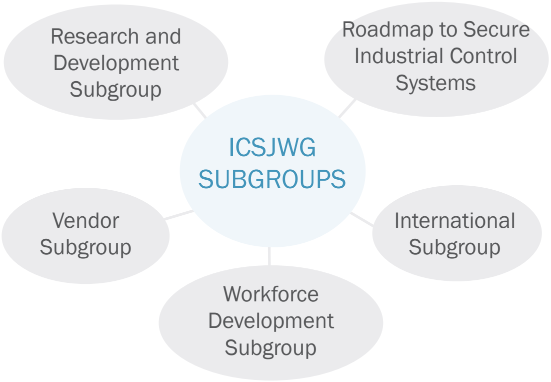
The ICSJWG operates under the National Infrastructure Protection Plan (NIPP) framework and Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The group's goal is to enhance the collaboration of ICS stakeholders by securing CIKR and accelerating the design, development, deployment, and secure operations of ICS.

The ICSJWG is a principle component of DHS's Strategy to Secure Control Systems, providing a coordinating body for sharing information and facilitating stakeholder efforts to manage cybersecurity risk.

Homeland Security

ICSJWG SUBGROUPS

The ICSJWG members have commissioned the following five subgroups.


ICSJWG SUBGROUPS
Research and Development Subgroup
Roadmap to Secure Industrial Control Systems
Vendor Subgroup
International Subgroup
Workforce Development Subgroup

THE INTERNATIONAL SUBGROUP will focus on enhancing international collaboration, knowledge sharing, and incident response by evaluating the challenges of sharing sensitive information between responsible national and government authorities.

THE RESEARCH AND DEVELOPMENT SUBGROUP will identify existing and planned R&D needs and priorities as they relate to industrial control systems and identify desired areas of ICS research not currently underway.

THE ROADMAP TO SECURE ICS SUBGROUP will maintain the Cross-Sector Roadmap to address cyber risk management within control systems environments and will coordinate its use.

THE VENDOR SUBGROUP will identify ways to improve information sharing between vendors, owners and operators, and other organizations involved in securing ICS.

THE WORKFORCE DEVELOPMENT SUBGROUP will continue to identify existing industrial control systems security curricula and make recommendations to enhance or create a new curriculum.

INTERNATIONAL

The International Subgroup addresses the growing need for international coordination to manage cyber risk in control systems environments both domestically and abroad. Key responsibilities include:

- Preparing a comprehensive "players" manual of international Computer Emergency Response Teams (CERTs) and their organization's contact and focus information;
- Preparing a communications plan for international collaboration;
- Documenting available collaboration tools, including a gap analysis to identify needed enhancements; and
- Identifying international document handling/ classification standards and performing a feasibility study to develop a common lexicon.

RESEARCH AND DEVELOPMENT

The Research and Development Subgroup facilitates communication between ICS stakeholders and the research and development community to ensure effective focus for research and development initiatives and associated funding. Key responsibilities include:

- Documenting current and planned projects with associated details, timelines, and stakeholders involved;
- Documenting results of an ICS research and development needs assessment; and
- Preparing a requirements document for sharing sensitive information, including an ultimate recommendation as to whether or not a new tool is needed.

ROADMAP TO SECURE INDUSTRIAL CONTROL SYSTEMS

The Roadmap to Secure ICS Subgroup creates a strategic plan to address the high-level management of cyber risk within control systems environments. The first version of the Roadmap was released in September 2011. Key responsibilities include:

- Documenting common threads for ICS challenges, priorities, and objectives across all infrastructure sectors for input to the ICS Roadmap;
- Performing a gap analysis to identify areas that need to be addressed; and
- Demonstrating a common vision and way-ahead for ICS security for all sectors.

VENDOR

The Vendor Subgroup addresses challenges and discusses issues related to managing risk associated with control systems products and services. The Subgroup also works to identify ways to improve collaboration and information sharing between vendors, owners, operators, and other organizations involved in securing ICS. Key responsibilities include:

- Developing white papers pertinent to the ICS community, including the Vulnerability Disclosure Paper and the Cross-Vendor Position White Paper;
- Documenting stakeholder groups, challenges, and equities; and
- Preparing recommendations that address all ICS groups and areas of concern.

WORKFORCE DEVELOPMENT

The Workforce Development Subgroup addresses challenges and priorities related to personnel awareness of cybersecurity issues within control systems environments and the development of skills for more effective cyber risk management. Key responsibilities include:

- Performing a gap analysis of control systems security workforce capabilities and development opportunities;
- Preparing a feasibility study for a control systems security certification program;
- Developing knowledge domain areas for a certification program; and
- Developing a control systems security workforce outreach plan.

ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

**For more information,
visit www.us-cert.gov/control_systems.**

CYBER SECURITY EVALUATION TOOL

PERFORMING A SELF-ASSESSMENT

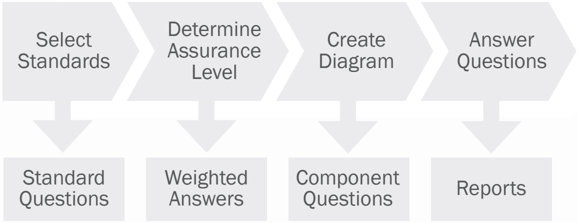
Control Systems Security Program

The Cyber Security Evaluation Tool (CSET^{TM}) is a self-contained software tool which runs on a desktop or laptop computer. It evaluates the cybersecurity of an automated, industrial control or business system using a hybrid risk and standards-based approach, and provides relevant recommendations for improvement. The Department of Homeland Security's (DHS) Control Systems Security Program (CSSP) developed the CSET application, and offers it to all through the United States Computer Emergency Readiness Team's (US-CERT) website.

HOW IT WORKS

CSET helps asset owners to assess their information and operational systems cybersecurity practices by asking a series of detailed questions about system components and architecture, as well as operational policies and procedures. These questions are derived from accepted industry cybersecurity standards.

Once the self-assessment questionnaire is complete, CSET provides a prioritized list of recommendations for increasing cybersecurity posture, including solutions, common practices, compensating actions, and component enhancements or additions. The tool also identifies what is needed to achieve a desired level of cybersecurity within a system's specific configurations.



THE ASSESSMENT PROCESS

All industry sectors can benefit from CSET's simple process for evaluating and improving their automated and industrial control systems (ICS) using these four basic steps.

1. SELECT STANDARDS

To get started, users are invited to select one or more of the following government and industry recognized cybersecurity standards. CSET then generates questions that are specific to those requirements.

- CFATS Risk Based Performance Standard (RBPS) 8: Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
- DHS Catalog of Control Systems Security: Recommendations for Standards Developers, Revisions 6 and 7
- DoD Instruction 8500.2 Information Assurance Implementation, February 2, 2003
- ISO/IEC 15408 revision 3.1: Common Criteria for Information Technology Security Evaluation, Revision 3.1
- NERC Reliability Standards CIP-002-009 Revisions 2 and 3
- NIST Special Publication 800-82 Guide to Industrial Control Systems Security, June 2011
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems Rev 3 and with Appendix I, ICS Controls
- NRC Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities, January 2010

Homeland Security

2. DETERMINE ASSURANCE LEVEL

The security assurance level (SAL) is determined by responses to questions relating to the potential consequences of a successful cyber attack on an ICS organization, facility, system, or subsystem. CSET then calculates a SAL and provides a recommended level of cybersecurity rigor necessary to protect against a worst-case event. Using the SAL to determine the required level of security, CSET runs a comparative analysis between the requirements identified in the standards selected and the answers provided by the user.

For assessments using the National Institute of Standards and Technology (NIST) standards and guidance, CSET also supports the Federal Information Processing Standards (FIPS) 199 guidelines for determining the security categorization of a system.

3. CREATE DIAGRAM

CSET contains a graphical user interface that allows one to diagram the control system network topology and identify the "criticality" of the network components. By creating a network architecture diagram, users are able to define the organization's cybersecurity zones, critical components, and communications conduits. An icon palette featuring various system and network components allows users to build diagrams by simply dragging and dropping them into place. Specific questions further facilitate the detailed identification of each component.

4. ANSWER QUESTIONS

CSET then generates questions using the network topology and selected security standards as its basis. The assessment team selects the best answer to each question using the organization's actual network configuration and implemented security policies and procedures. The tool compares the completed answers with the recommended requirements from the standards and generates a list of recognized good practices and security gaps. CSET also generates both interactive (on-screen) and printed reports. The reports provide a summary of security level gaps or areas that did not meet the recommendations of the selected standards. The assessment team may then use this information to plan and prioritize mitigation strategies.

CSET AT-A-GLANCE

Over the past few years, CSSP has assisted with numerous onsite self-assessments across the country and in all critical infrastructure sectors. In 2011, ICS owners and operators downloaded more than 1,600 copies of CSET and CSSP helped perform 81 self-assessments in 26 states. Sectors with the highest number of self-assessments include: water and water treatment, energy, transportation, commercial and government facilities, and public health/healthcare.

The CSSP team observed that the most common vulnerabilities identified through CSET self-assessments were a lack of adequate control system inventories and formal documentation; no audit capabilities and accountability for event monitoring; and missing permissions, privileges, and access control restrictions. Other categories of vulnerabilities included improper authentication and credentials management practices, flaws in network architecture designs, configuration (implementation) settings within network components, and traceability on cybersecurity configuration and maintenance.

To assist an organization in planning for a CSET self-assessment, key staff should become familiar with information about the organization's ICS components, understanding the complete list of assets, including all operational hardware assets and components, as well as software for all user interfaces. Staff should also understand data exchanges and operational data flow. To adequately prepare for a CSET self-assessment, staff should review policies and procedures, network topology diagrams, inventory lists of critical assets and components, risk assessments, IT and ICS network policies and practices, and organizational roles and responsibilities.

GETTING STARTED

Get started by downloading CSET at www.us-cert.gov/control_systems/csetdownload.html.

To learn more about CSET or to request a CD copy of the software, contact cset@dhs.gov.

For general program questions or comments, contact cssp@dhs.gov
or visit www.us-cert.gov/control_systems.

ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

For more information,
visit www.us-cert.gov/control_systems.

Control Systems Security Program

ONSITE CONSULTATION AND SELF-EVALUATION

The Department of Homeland Security's (DHS) Control Systems Security Program (CSSP) assists owners of networks and industrial control systems (ICS) in assessing and strengthening their organization's cybersecurity posture. Through a tiered system including the Cyber Security Evaluation Tool (CSET™) and onsite consultation options, CSSP helps ICS asset owners take the preventative measures necessary to prepare for and protect from cyber attacks.

CUSTOMIZABLE SUPPORT

With the increasing threat of cyber attacks, CSSP is seeking to expand awareness of defense-in-depth strategies for cybersecurity. A tiered approach allows asset owners and operators to select the level of CSSP support needed to meet their operational needs.

Onsite consultations are offered at no cost to asset owners and provide an opportunity to examine organizations' cybersecurity posture with the assistance of DHS's cybersecurity subject matter experts.

CSSP TIERED APPROACH

CSET Self-Assessment

Tier 1: CSET System and Process Evaluation

Tier 2: Network Architecture Review

CSET SELF-ASSESSMENT

The CSET is a self-contained software tool which runs on a desktop or laptop. Asset owners can leverage the CSET application to evaluate the cybersecurity posture of an automated, industrial control or business system. CSET uses a hybrid risk and standards-based approach, and provides relevant recommendations for improving the security of an organization. CSSP developed the CSET application, and offers it to all through the Control Systems Security Program website.

TIER 1 – CSET SYSTEM AND PROCESS EVALUATION

Tier 1 offers an onsite consultation provided by CSSP cybersecurity staff at asset owners' facilities. The asset owners leverage the CSET application, while receiving technical guidance from the CSSP consultation team.

The Tier 1 consultation focuses on identifying the primary vulnerabilities and improvements for asset owners using industry recognized cybersecurity standards as the basis for performance. Tier 1 consultations are typically conducted in one day with one or two of CSSP's experienced subject matter experts, along with the asset owners and key staff. The consultation provides a quick and effective analysis of the control system and its core functions, infrastructure, and policies and procedures. A Tier 1 consultation is generally sufficient for assets that support most critical facilities and infrastructures.

TIER 2 – NETWORK ARCHITECTURE REVIEW

Tier 2 consultation offers a network architecture review and analysis, which can be completed independent of, or in conjunction with, a CSET self-assessment or system and process evaluation. The network architecture review includes a comprehensive evaluation and discovery process, focusing on defense strategies associated with asset owners' specific control systems network. This process may include an in-depth review and evaluation of control systems network design, configuration and application.

Homeland Security

The Tier 2 assessment, like Tier 1, is conducted onsite by the asset owners with the support of CSSP cybersecurity professionals. However, the Tier 2 consultation provides a more robust evaluation of system interdependencies, vulnerabilities, and mitigation options. This consultation typically requires additional rigor and technical staff and often takes two to three days to complete. As part of the review, experts examine information related to key control systems external connections and conduct an extensive review of control system design documents, drawings, and architectures. This assessment is likely to be useful for most high-security control systems, such as chemical, power and nuclear plants, telecommunications facilities, government facilities, schools, hospitals, and other high-value infrastructure assets.

CROSS-FUNCTIONAL COOPERATION

In order to garner the most accurate and useful results from the CSET application and CSSP onsite consultations, coordination with subject matter experts from across the ICS organization is vital. This cross-functional team often consists of representatives from the operational, maintenance, information technology, business, and security divisions. The organization's team can prepare to participate in a CSET self-assessment or CSSP onsite consultation by reviewing their policies and procedures, network topology diagrams, inventory lists of critical assets and components, risk assessments, and organizational roles and responsibilities.

CONSULTATION PREPARATION

When planning and organizing for an onsite consultation, the following is recommended:

- Identify the cross-functional assessment team members from your organization and schedule a date.
- Ensure cross-functional assessment team members have reviewed relevant information and are adequately prepared to participate in the consultation session.
- Select a meeting location to accommodate the consultation team during the question and answer portion of the assessment.

BENEFITS OF CSSP SUPPORT

By leveraging the CSET application and CSSP onsite consultation opportunities, asset owners can increase the cybersecurity posture of their organization. Some key benefits include:

- Highlighting vulnerabilities in the organization's systems and providing recommendations on ways to address them;
- Identifying areas of strength and recommended practices being followed in the organization;
- Providing a method to systematically compare and monitor cyber systems improvement;
- Informing an organization's risk management and decision-making process; and
- Raising awareness and facilitating discussion on cybersecurity within the organization.

REQUEST CSSP SUPPORT

To learn more about CSET or to download a copy, visit www.us-cert.gov/control_systems.

To request a Tier 1 or Tier 2 onsite consultation, send an email to cset@dhs.gov.

For general program questions or comments, contact cssp@dhs.gov.

ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

**For more information,
visit www.us-cert.gov/control_systems.**

Control Systems Security Program

TRAINING

The Control Systems Security Program (CSSP) training courses and workshops share in-depth defense strategies and up-to-date information on cyber threats and mitigations for vulnerabilities with the goal of improving cybersecurity preparedness in the control systems community.

WEB-BASED TRAINING

OPSEC FOR CONTROL SYSTEMS: Intended to provide an overview of operations security for industrial control systems (ICS), which are also referred to as supervisory control and data acquisitions (SCADA), distributed control systems (DCS), and process control systems (PCS).

CYBERSECURITY FOR CONTROL SYSTEMS ENGINEERS & OPERATORS: Intended for control system employees whose primary job is not cybersecurity.

INSTRUCTOR-BASED TRAINING

INTRODUCTION TO INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY (101)—8 HOURS

Students learn the basics of ICS security, including information on security vulnerabilities and mitigation strategies unique to the control system domain, and a comparative analysis of Information Technology (IT) and control system architecture.

The course is split into six sessions: (1) Industrial Control System Overview; (2) Process Control Exploit Demonstration; (3) Network Discovery and Mapping; (4) Exploiting Vulnerabilities; (5) Network: and (6) Defense, Detection, and Analysis.

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY FOR MANAGEMENT (111)—2 HOURS

Tailored to managers, this course provides a basic understanding of control systems and the current ICS cybersecurity threat landscape. The session includes a discussion of how the risk equation can be used to prioritize the actions needed to mitigate vulnerabilities and monitor ICS.

INTERMEDIATE CYBERSECURITY FOR INDUSTRIAL CONTROL SYSTEMS (201)—LECTURE ONLY—8 HOURS

This course helps students understand how cyber attacks are launched and why they work. The session also covers mitigation strategies that can be used to increase the cybersecurity posture of ICS. This class is a prerequisite for Intermediate Cybersecurity for Industrial Control Systems (202) with lab and exercises.

This course is split into four sessions: (1) Current Security in ICS, (2) Strategies Used Against ICS, (3) Defending the ICS, and (4) Preparation and Further Reading.

INTERMEDIATE CYBERSECURITY FOR INDUSTRIAL CONTROL SYSTEMS (202) WITH LAB AND EXERCISES—8 HOURS

This course provides a brief review of ICS security; with a focus on how attacks against ICS are launched and why they work. Mitigation strategies are also covered in depth.

Throughout this hands-on class, a sample process control network is used to demonstrate various exploits that can be used to gain unauthorized control of a system. Working with the sample network during class exercises helps students to understand mitigation techniques and develop control systems cybersecurity skills they can apply to their jobs.

Homeland Security

This course is split into six sessions: (1) Supervisory Control and Data Acquisition and Control System Overview; (2) Risk to Industrial Control Systems; (3) Exploit Demonstration; (4) Basic Control Security Considerations; (5) Network: Security, Identification, and Remediation; and (6) Network: Defense, Detection, and Analysis.

ICS ADVANCED CYBERSECURITY (301)— 5 DAYS

Intensive hands-on training in protecting and securing ICS from cyber attacks, this session includes a Red Team/Blue Team exercise conducted within an actual control systems environment. The exercise presents an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

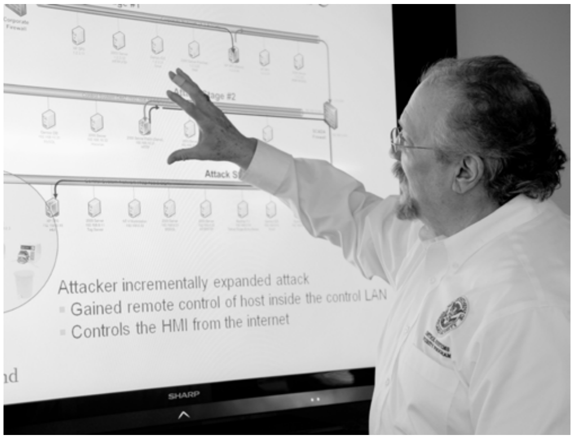
DAY 1—Welcome; overview of the DHS Control Systems Security Program; brief review of cybersecurity for ICS; demonstration of how a control system can be attacked from the Internet; hands-on classroom training on Network Discovery techniques and practices.

DAY 2—Hands-on classroom training on Network Discovery and Metasploit; separating into Red and Blue Teams.

DAY 3—Hands-on classroom training on Network Exploitation and Network Defense techniques and practices; Red and Blue Team strategy meetings.

DAY 4—A 12-hour Red Team/Blue Team exercise. The Blue Team is tasked with providing the cyber defense for a corporate environment and with maintaining operations to a batch mixing plant and an electrical distribution SCADA system. The Red Team attempts to attack the Blue Team's systems.

DAY 5—Red Team/Blue Team exercise lessons learned and roundtable discussion.


Attacker incrementally expanded attack
Gained remote control of host inside the control LAN
Controls the HMI from the internet
SHARP

PREREQUISITES: Each attendee should have practical knowledge with ICS networks, software, and components; have basic coding skills; and a fairly deep understanding of IT network details, such as the difference between UDP and TCP protocols, and MAC and IP addresses.

Every student attending this course should bring a laptop computer (with a DVD drive) in which they have "administrator" privileges allowing them to configure and load software.

OBTAINING ADDITIONAL INFORMATION

To learn more about these training sessions contact cssp_training@hq.dhs.gov.

For a list of upcoming training events visit www.us-cert.gov/control_systems/cscalendar.html.

For general program questions or comments contact cssp@dhs.gov or visit www.us-cert.gov/control_systems.

ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

For more information, visit www.us-cert.gov/control_systems.