# 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.

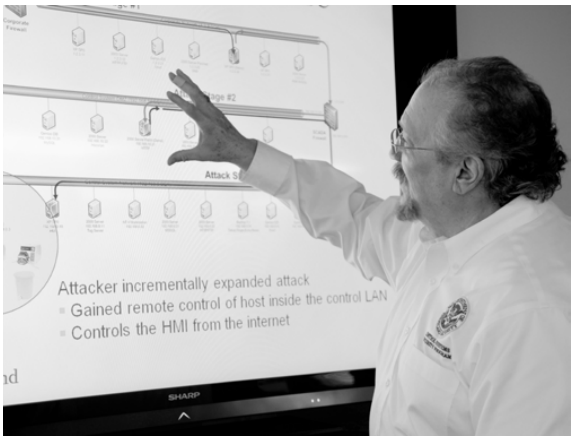
**DAY 1**—Welcome; overview of the DHS Control Systems Security Program; brief review of cybersecurity for ICS; demonstration of how a control system can be attacked from the Internet; hands-on classroom training on Network Discovery techniques and practices.

**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.




**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.**