# Cybersecurity Training for Industrial Control Systems

The United States Department of Homeland Security Control Systems Security Program and the Cybersecurity and Infrastructure Security Agency (CISA) is pleased to offer Cybersecurity for Industrial Control Systems. There is no fee to attend the courses. Accommodations, time, travel, and food are the responsibility of the individual attendee.

### Who Should Attend

This live training is provided specifically for personnel responsible for the oversight, design, and operation of control systems. This includes operators, engineers, IT personnel, supervisors, emergency managers, and managers.

**Prerequisite: Every student attending the courses must bring a laptop computer (no tablets) with wireless capability (to connect to the internet and exercise networks) and a minimum of 8GB of RAM. A modified Kali distribution containing additions to support classroom exercises will be used during the course along with a modified Security Onion VM. Each student must arrive with a VMware® software virtualization package (Workstation, Player, or Fusion) installed on their laptop. You must have administrator privileges to install the VM player.**

## EVENT DETAILS

**DATES** February 22nd-25th, 2022

**TIME** 8:00 am to 5:00pm
Including 1hr lunch

**LOCATION** Kentucky Transportation Cabinet Conference Center
200 Mero Street
Frankfort, KY 40622

**FREE REGISTRATION**
Please register for this event at:
https://region4-ics-cybersecuritytraining.eventbrite.com

## Course Description:

**Tuesday, February 22nd, 8:00 am – 12:00 pm**
**Introduction to Control Systems Cybersecurity (101):**
The purpose of this course is to introduce students to the basics of industrial control systems security. There will be opportunities to take part in several online lab exercises to become more familiar with control system concepts. The training includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain. A look at critical infrastructure dependencies will also be addressed.

**Tuesday, February 22nd, 1:00 pm – 5:00 pm**
**Cyber Security Evaluation Tool (CSET):** This exercise will demonstrate the primary functionality of CSET. Participants will walk through short examples on how to use the tool to perform a self-evaluation of a system. CSET is useful to self-evaluate against a number of industry standards. It can be very helpful in benchmarking how a company currently meets the selected standards and then tracking improvements, through the aid of scoring, customizable graphs, and charts. This tool includes a Visio-like drawing capability to create a network diagram with digital components to aid in documentation.
CSET is available for free download. https://github.com/cisagov/cset

**Wednesday, February 23rd, 8:00 am – 5:00 pm**
**Intermediate Cybersecurity for Industrial Control Systems, Lecture Part 1 (201):** This course provides technical instruction on the protection of industrial control systems using offensive and defensive methods. Students will understand how cyber-attacks could be launched, why they work, and mitigation strategies to increase the cybersecurity posture of their control system. Demonstrations will include the use of software tools to establish a baseline of your network(s), and to monitor and analyze its traffic.

***Two courses will be presented alternately on Thursday and Friday, with 25 seats available for each class. Students will have the option to select which day they would prefer to take each course.**

**Thursday, February 24th and Friday February 25th 8:00 am – 5:00 pm**
**Intermediate Cybersecurity for Industrial Control Systems, Part 2 (202) Hands-on:**
Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample process control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the many hands-on exercises that will help the students develop control systems cybersecurity skills they can apply when they return to their jobs.

**Thursday, February 24th and Friday February 25th 8:00 am – 5:00 pm**
**CyberStrike: Hands-on workshop for defending against an OT cyberattack**
**[No laptop required]** This course offers a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine. The instruction platform challenges course participants to defend against a cyberattack on the equipment they routinely encounter within their industrial control systems.

## Questions:

For additional information please contact:

**Colin Glover**
Cybersecurity Advisor – Kentucky (Region 4)
DHS Cybersecurity and Infrastructure Security Agency (CISA)
Colin.glover@cisa.dhs.gov

Or

**Russell Gold**
Idaho National Laboratory
Cybersecurity Analyst/Instructor
Russell.gold@inl.gov

**For additional scheduled ICS events see**:
https://us-cert.cisa.gov/ics/Calendar