Homeland Security

August 6 – 9, 2019

Cybersecurity Training for Industrial Control Systems

The United States Department of Homeland Security Control Systems Security Program is pleased to offer Cybersecurity for Industrial Control Systems.

When: August 6 - 9, 2019

Where: Denver Federal Center
Building 25
Kipling St., Denver, CO 80225

Registration: Please register for this training at
https://secure.inl.gov/reg0819
There is no fee to attend these courses.
For other scheduled events see
https://secure.inl.gov/Calendar.

Who Should Attend: This 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.

Course Descriptions:

Tuesday, August 6, 8:00 am – 5:00 pm

Introduction to Control Systems Cybersecurity (101): The purpose of this course is to introduce students to the basics of industrial control systems security. This includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

Tuesday, August 7, 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.

Wednesday, August 8th and Thursday August, 9th 8:00 am – 5:00 pm

Two courses will be presented alternately on Wednesday and Thursday, with 50 seats available for each class.

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.

Prerequisite: **Every student attending the Intermediate Part 2 (202) course must bring a laptop computer (no tablets) with wireless capability (to connect to the 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. 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.**

CyberStrike: – Lessons learned and walkthrough of the Black Energy attack on the Ukraine. [No laptop required]
This course offers a hands-on, simulated demonstration of a cyberattack, drawing form 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 email ICSTraining@inl.gov