

Introductory Industrial Control Systems Security (ICS) Security (4 hours)

This course is being offered Monday July 12, 2010 from 1:00 – 5:00 PM, prior to the NITSL Workshop.

All registered attendees of the NITSL Workshop are welcome to attend.

If you plan on attending, send an email to the NITSL Program Manager, Gregory.Przyjemski@TRMnet.com, indicating that you plan to attend the training.

Who should attend:

System managers and control operators for power and energy generation, transmission and distribution organizations.

Description:

The DHS Control Systems Security Program is please to offer this fast-paced course that will cover general control systems cyber security challenges.

The training objectives include:

- Looking at the risk equation (threat, vulnerability and consequences) and how they relate to the control system environment.
- Who are the threat actors?
- What vulnerabilities exist in the control systems space?
- What can be the consequences of exploitation?
- What mitigation strategies can be implemented to help protect the control system environment?
- A program overview of the DHS Control Systems Security Program

This is a lecture course with a video demonstration of how an attack can be launched against a control system environment.

A note from the instructor:

My name is Jonathan Gray; I am one of the members of the Department of Homeland Security's Control Systems Security Program. This course is structured to help students not only understand exactly how attacks against Industrial Control Systems (ICS) can be launched and why they work, but also provides mitigation strategies to increase the cyber security posture of your control system network.

Instructor Bio



Jonathan Gray

Critical Infrastructure Protection/Resilience

Jonathan Gray is an instrument and controls system engineer in the Control Systems Security Program for the Department of Homeland Security Control Systems Security Program at INL. He has over 14 years of instrumentation and controls experience in industrial automation ranging from capital projects to contracting, technical training, and support. He has performed work for mining, refining, specialty chemicals, food, pharmaceuticals, prisons, terminal facilities, and pipelines.