CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG

INDUSTRIAL CONTROL SYSTEMS
JOINT WORKING GROUP

New ICS Cybersecurity Educational Opportunities

CISA hosts the ICSJWG to ensure a variety of ICS stakeholders have opportunities to improve their cybersecurity posture and education. ICSJWG is pleased to announce a new CISA hosted ICS training program facilitated by Idaho National Laboratory (INL). This training program has been integrated with the ICS CYBER-CHAMP© educational maturity model to produce two new ICSJWG training tracks—foundational and advanced. A presentation was provided to explain CYBER-CHAMP© during the Fall 2020 Virtual Meeting session.

ICS CYBERsecurity—Competency Health And Maturity Progression model CYBER-CHAMP©

A model for measuring and improving organizational ICS Cybersecurity Operational Readiness, providing types of training, and learning paths to ensure individual job roles and responsibilities are known and carried out securely. This presentation was offered on September 22, 2020.

Fall 2020

The dual-track ICS cybersecurity educational breakout sessions for Fall 2020 will include two foundational and two advanced sessions. Each session starts at 10am MST and is expected to be ~50 minutes:

Foundational:

Session 3—Cybersecurity Differences within IT and ICS Domains: Introduces the differences between IT and ICS Domains. Topics include: generations of ICS; communication, operations, and support differences; why ICS domains should be separate from IT domains.
This session will be on September 28. Please register at: https://attendee.gotowebinar.com/register/8999962678704034575

Session 4—Cyber Risks to ICS: Introduces Cyber Risks to ICS systems. Topics include: Risk Curve; threat trends; adversarial risk, OSINT, OPSEC, and supply chain risks; basics to determine ICS critical cyber risk. The risks outline the importance of understanding your network and why ICS networks are different than IT networks.
This session will be on October 5. Please register at: https://attendee.gotowebinar.com/register/1519949890571976463

Advanced:

Session 9—Analyze Previously Captured ICS Traffic to Discover Vulnerabilities: Introduces tools to analyze previously captured ICS traffic. Topics include: determining data flow; kind of remote access used; knowing what is coming in and out of your network. Open source tools will be available for everyone to use.
This session will be on October 12. Please register at: https://attendee.gotowebinar.com/register/5999371257247768591

Session 10—Assessing Wireless Vulnerabilities in an ICS Environment: Discussion on high-level wireless communications. Topics include: IEEE 802.11 Protocols (Wi-Fi), IEEE 802.15 Protocols and a quick intro to 5G Protocols. We will look at a few wireless packet capture tools.
This session will be on October 19. Please register at: https://attendee.gotowebinar.com/register/6679158614771526159

If you missed Sessions 1, 2 7, or 8, they are available at: https://ics-training.inl.gov

Additional foundational and advanced sessions will be made available during upcoming ICSJWG meetings. Possible foundational topics may include Critical Infrastructure Sector Dependances and exploits in ICS infrastructure. Advanced topics may include: Manipulate IDS Logs using Elastic Stack and Explain, Identify, and Evaluate ICS.