Control Systems Cybersecurity Resource, Training & Education Guide

Air Force Control Systems Community
https://go.usa.gov/xNwAa

Air Force Office of the Chief Information Security Officer
https://go.usa.gov/xNwAC

SAF/CIO A6 SharePoint
https://go.usa.gov/xNwAr

Civil Engineering Portal
https://go.usa.gov/xNwAg

DHS ICS-CERT
https://ics-cert.us-cert.gov/

US CYBERCOM
https://go.usa.gov/xNwAK

Risk Management Framework Knowledge Service
https://go.usa.gov/xNwA9

Information Assurance Support Environment
https://go.usa.gov/xNwA5
https://go.usa.gov/xNwAN

Force Development

INSTRUCTOR-LED TRAINING (DHS ICS-CERT)

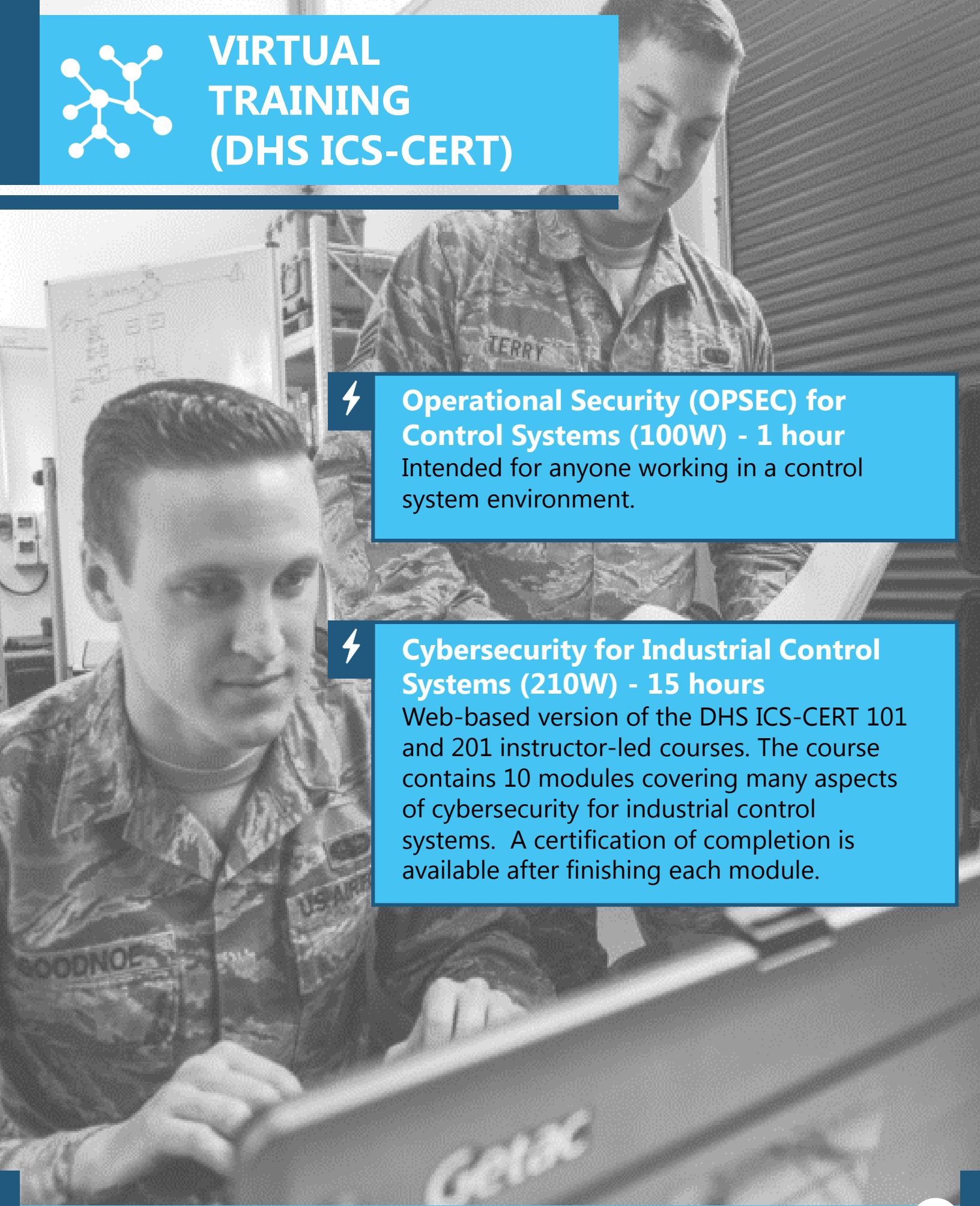
Introduction to Control Systems Cybersecurity (101) - 1 day
To introduce students to the basics of industrial control systems security. This includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

Intermediate Cybersecurity for Industrial Control Systems (201) (lecture only) - 1 day
To provide 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 networks. In addition, this course acts as a prerequisite for the next course (DHS ICS-CERT 202).

Intermediate Cybersecurity for Industrial Control Systems (202) (with lab/exercises) - 1 day
To provide a brief review of industrial control systems security, including a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain. 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 hands-on exercises that will help the students develop control systems cybersecurity skills they can apply in their work environment.

ICS Cybersecurity (301) - 5 days
To provide in-person, hands-on training to discover who and what is on the network, identify vulnerabilities, learn how those vulnerabilities may be exploited, and learn defensive and mitigation strategies for control system networks. The week includes a Red Team / Blue Team exercise that takes place within an actual control systems environment and provides the opportunity to network and collaborate with other colleagues involved in operating and protecting control system networks.

VIRTUAL TRAINING (DHS ICS-CERT)



Operational Security (OPSEC) for Control Systems (100W) - 1 hour

Intended for anyone working in a control system environment.

Cybersecurity for Industrial Control Systems (210W) - 15 hours

Web-based version of the DHS ICS-CERT 101 and 201 instructor-led courses. The course contains 10 modules covering many aspects of cybersecurity for industrial control systems. A certification of completion is available after finishing each module.

More Info: https://ics-cert-training.inl.gov/lms/

AIR FORCE / DoD EDUCATION AND TRAINING

Air University - Cyber College
The Air Force Cyber College focuses on the education and research required to provide the AF cyber community with cutting-edge solutions to their problems. This research is an integral part of the graduate education at Air University and the AF workforce, and provides students with creative, meaningful thesis and dissertation topics. http://www.airuniversity.af.mil/CyberCollege/

Air Force Institute of Technology (AFIT) - Center for Cyberspace Research (CCR)
The CCR, established in March 2002, conducts defense-focused cybersecurity research at the Master's and PhD levels. The CCR is a national Center of Academic Excellence in Cyber Defense Research, as designated by the Department of Homeland Security and the National Security Agency. AFIT is also an NSA-designated Center of Academic Excellence in Cyber Operations. https://www.afit.edu/CCR/

National Defense University (NDU) - College of Information and Cyberspace
The NDU is a national security institution focused on advanced joint education and leader development and scholarship. The NDU College of Information and Cyberspace educates and prepares selected military and civilian leaders and advisers to develop and implement cyberspace strategies, and to leverage information and technology to advance national and global security. http://cic.ndu.edu/

DISA Information Assurance Support Environment (IASE)
The IASE provides one-stop access to cybersecurity information, policy, guidance, and training for cybersecurity professionals throughout the DoD. These resources are provided to enable the user to comply with rules, regulations, best practices, and federal laws. http://iase.disa.mil/eta/Pages/index.aspx

A4C Force Development –
Vigilance: Cybersecurity of Control Systems Documentary
The A4C Force Development team captured insight from seven subject matter experts to create a one-hour documentary on the growing cybersecurity threats to control systems, the potential risk to the Air Force mission, and cyber hygiene best practices to protect Air Force installations from cybersecurity attacks. https://go.usa.gov/xNApt

EXTERNAL TRAINING

COMMERCIAL TRAINING

- **SANS ICS410**: ICS/SCADA Security Essentials https://www.sans.org/course/ics-scada-cyber-security-essentials
- **SANS ICS515**: ICS Active Defense and Incident Response https://www.sans.org/course/industrial-control-system-active-defense-and-incident-response
- **SCADAHacker**: Understanding, Assessing and Securing Industrial Control Systems (40-80 hours) https://scadahacker.com/training.html

INDUSTRY CERTIFICATIONS

- **(ISC)² Certified Information Systems Security Professional (CISSP)** https://www.isc2.org/cissp/default.aspx
- **Global Industrial Cyber Security Professional (GICSP) Certification** https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp
- **INFOSEC Institute: Certified SCADA Security Architect (CSSA)** http://www.iacertification.org/cssa_certified_scada_security_architect.html

NOTE:

The U.S. Department of Defense Directive 8570.1 requires every full and part-time military service member, defense contractor, civilian and foreign employee with "privileged access" to a DoD system, regardless of job series or occupational specialty, to obtain a commercial certification credential that has been accredited by the American National Standards Institute (ANSI). See the complete approved baseline certification matrix here: http://iase.disa.mil/iawip/Pages/iabaseline.aspx