**Critical Infrastructure Cybersecurity**

**Course Description:**

Students will address basic security concepts as they apply to critical infrastructure systems. Concepts addressed in the course will include Industrial Control Systems (ICS), such as Supervisory and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), national standards for the protection of critical infrastructure, and risk management concepts and tools for critical infrastructure systems. Students will perform a risk assessment of a specific critical infrastructure sector using an appropriate risk assessment framework and tools, identifying threats and vulnerabilities specific to the sector, and making appropriate recommendations for mitigating risk.

**Prerequisites:**

Students should have completed an introductory security course, such as CompTIA’s Security+, or otherwise have knowledge of basic network and computer security concepts and technologies.

**Technology Requirements:**

Students must be able to access and subscribe to the FEMA education portal (https://training.fema.gov/) and the ICS-CERT education portal (https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT).

Students are also required to have the following computer minimum requirements:

***(information should be provided by instructor)***

**Course Objectives:**

Topics addressed in the course include:

* Critical infrastructure (CI) and critical infrastructure security and resilience (CISR), including the 16 CI sectors, as defined by the Department of Homeland Security (DHS) and identified in Presidential Policy Directive 21 (PPD-21: Critical Infrastructure Security and Resilience).
* Industrial Control Systems (ICS) such as SCADA, PCS, and DCS.
* Risk management frameworks applicable to CI systems.
* Cybersecurity services, such as confidentiality, integrity, availability, and authentication, as they apply to critical infrastructure systems.
* Cybersecurity threats, risks, vulnerabilities, and attacks as they apply to CI systems.
* Vulnerability assessments and tools applicable to CI systems.
* CI systems risk management strategies.
* Trends in cybersecurity impacting CI sectors.

**Student Outcomes:**

At the conclusion of the course, students will be able to:

* Define CI sectors and identify legislation and standards addressing CI protection.
* Define common terms and concepts associated with CI, including ICS, SCADA, PCS, and DCS.
* Identify the components and process of implementing a CISR risk management program.
* Describe cybersecurity services such as confidentiality, integrity, availability, and authentication as they apply to critical infrastructure systems.
* Select appropriate vulnerability assessment frameworks and tools as a part of a risk assessment of a CI system.
* Identify and describe cybersecurity threats, risks, vulnerabilities, and attacks as they apply to CI systems.
* Identify an appropriate risk management strategy for CISR.

**Module 1. Introduction to Critical Infrastructure**

**Description:** This module covers the Critical Infrastructure Security and Resilience foundational courses and certifications from the Federal Emergency Management Administration (FEMA). It is based on a four-part assignment that uses the online FEMA Emergency Management Institute courses and exam certifications that will cover the following four topics:

1. IS-821.A: Critical Infrastructure Support Annex

2. IS-860.C: The National Infrastructure Protection Plan, An Introduction

3. IS-913.A: Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration

4. IS-921.A: Implementing Critical Infrastructure Security and Resilience

The focus is on five key subject sectors that the National Infrastructure Protection Plan identifies as “Lifeline” sectors: Energy, Water and Wastewater Systems, Communications, Transportation Systems, and Emergency Services. This module gives students a better understanding of what those assets are, what components are considered “critical,” and how to identify them for entry into the IP Gateway that serves as the single interface through which Department of Homeland Security (DHS) partners can access the department’s integrated infrastructure protection tools and information.

**Module Objectives:**

* Define critical infrastructure, protection, and resilience in the context of the National Infrastructure Protection Plan (NIPP).
* Describe critical infrastructure in communities and the impact Lifeline sector assets have on a community’s resiliency.
* Describe the processes that support critical infrastructure security and resilience.
* Identify strategies and methods for achieving results through critical infrastructure partnerships.
* Describe the roles and responsibilities of entities such as the DHS, sector-specific agencies, and state, local, tribal, and territorial governments.
* Discuss common standards bodies, such as the North American Electricity Reliability Council (NAERC) and the National Institute of Standards and Technology (NIST).
* Understand which certifications are required to protect critical infrastructure.

**Required Reading:** Miller, Stephen, and Clark, Richard H. Framework for SCADA Cybersecurity. Smashwords Edition, eBook ISBN 978-1310-30996-0. Chapter 2 “Cybersecurity Framework Introduction,” Section 1 “Framework Introduction,” pages 43-45. Available at https://www.smashwords.com/books/view/510004.

**Hands-on Activity:** This four-part assignment uses the online FEMA Emergency Management Institute courses and exam certifications that cover four topics. The focus is on five key subject sectors that the National Infrastructure Protection Plan identifies as “Lifeline” sectors

**Team Activity**: Students pair into teams, which identify one of the 16 critical infrastructure sectors to focus on throughout the course. Each week’s lesson will be examined through the lens of the chosen sector. Student teams are expected to investigate their chosen sector and create a fictitious organization that will be used as a case study in future assignments.

**Module 2. Introduction to Control Systems and SCADA**

**Description:** This module introduces Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Process Control Systems (PCS), with overviews of what they are and how they are used.

**Module Objectives:**

* Describe the components and applications of industrial control systems.
* Describe the purpose and use of SCADA, DCS, and PCS systems.
* Describe the configuration and use of field devices used to measure critical infrastructure processes, such as flow rate, pressure, temperature, level, density, etc.
* Describe the use and application of Programmable Logic Controllers (PLCs) in automation.

**Hands-on Activity:** Students download a 15-day free trial of PLC Ladder (located at PLCtrainer.net or LogicsPro). They install the software and explore its options to understand how PLC works; packet capture – protocol and transit across the network; and how to program the PLC. ***Your instructor will provide additional assignment details.***

**Team Activity**: Student teams continue to build a description of the operating environment for their sector-based organizations. What systems will be used within the organization?

**Module 3. Technologies**

**Description:** A number of different networking and SCADA protocols, hardware, and security devices are available to protect a network and the devices on that network. This module addresses the various mechanisms for employing hardware, protocols, and technologies with basic protections in infrastructure and network design. It also identifies methods for enhancing the security of an enterprise network through the positioning of certain pieces of hardware, protocol, and network equipment.

**Module Objectives**

* List several types of networking hardware and explain the purpose of each.
* List and describe the functions of common communications protocols and network standards used within CI.
* Identify new types of network applications and how they can be secured.
* Identify and understand the differences between IPv4 and IPv6.
* Discuss the unique challenges/characteristics of devices associated with industrial control systems.
* Explain how existing network administration principles can be applied to secure CIKR.

**Required Reading:** Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Department of Homeland Security. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. September 2016. Available online at https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP.

**Hands-on Activity:** Explore the interactive graphic Secure Architecture Design. This secure design is the result of an evolutionary process of technology advancement and increasing cyber vulnerability presented in the Recommended Practice document Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ***Your instructor will provide additional assignment details.***

**Team Activity**: Student teams continue to build a description of the operating environment for their sector-based organizations. They identify the networking protocols and technologies that will be used within the organization.

**Module 4. Risk Management**

**Description:** This module covers cybersecurity critical infrastructure and risk management. It introduces the NIST Cybersecurity Framework, the structure of the framework, and how it is used. It also describes the processes of risk management in the framework—framework basics, structure, and a business process management approach to implementing and applying the framework.

**Module Objectives**:

* Describe basic security service principles (confidentiality, integrity, availability, and authentication) and their relative importance to CI systems.
* Explain basic risk management principles.
* Identify various risk management frameworks and standards, such as the NIST Cybersecurity Framework and the North American Electricity Reliability Council (NERC).
* Describe how to use the framework core process.
* Describe how to use the Framework Implementation Tiers to identify cybersecurity risk and the processes necessary to effectively manage that risk.
* Describe the Cybersecurity Framework Assessment Process Model.
* Demonstrate an understanding of how the framework process holistically manages risk.

**Team Activity**: Student teams continue to build a description of the operating environment for their sector-based organization. They select an appropriate risk management framework for the sector-based organization. In the absence of one required by the industry, teams should begin to apply the NIST Cybersecurity Framework to the selected organization. Each team’s work should be reviewed by the instructor.

**Module 5. Threats**

**Description**: In this module, we will examine common attacks against CI including, hi-jacking, denial of service attacks, malicious software, SMTP spam engines, Man-in-the-Middle (MITM), and social engineering. The module will explore how attacks through users are being conducted today and the different kinds of attacks that target server-side and client-side applications. Then, it explores some of the common attacks that are launched against networks, CI and SCADA/Control Systems and other CI devices today. This example provides an overview of how malware like Stuxnet impact SCADA systems. We will look at how these malware are designed, configured, and how they work. We look at the current and future impact of these malware on SCADA systems.

**Module Objectives**:

* Define threats and threat agents, and explain how risk assessment relates to understanding threats.
* Identify how different threats—including hijacking, denial-of-service attacks, malicious software, SMTP spam engines, Man-in-the-Middle (MITM) attacks, and social engineering—would apply to critical infrastructure.
* Identify different types of malware and their intended payloads.
* Describe social engineering psychological attacks.
* List and explain the different types of server-side web application and client-side attacks relevant to critical infrastructure.
* Describe overflow attacks and provide examples of the impact on CI systems.
* Provide examples of malware attacks, such as Flame, Stuxnet, BlackEnergy, Havex, and Duqu, and discuss their functionality and impact on critical infrastructure systems.

**Required Reading:** U.S. Government Accountability Office (GOA). *Critical Infrastructure Protection: Cybersecurity Guidance Is Available But More Can Be Done to Promote Its Use.* GAO-12-92. Published: December 9, 2011. Publicly released: January 9, 2012. Available online at http://www.gao.gov/products/GAO-12-92.

**Team Activity**: Student teams continue to build descriptions of the operating environment for their sector-based organizations. They review the different threat possibilities using the Government Accountability Office (GAO) table, “Sources of Emerging Cybersecurity Threats.” Teams identify the different threats that would be likely to impact their sector-based organizations, providing a rationalization for their selections.

**Module 6. Vulnerabilities**

**Description:** Vulnerabilities are weaknesses that enable threats to be actualized. This module discusses cybersecurity vulnerabilities in general and those that are of a higher concern for critical infrastructure systems. It also identifies processes and tools for discovering vulnerabilities.

**Module Objectives**:

* Identify the common vulnerabilities associated with Control Systems (CS).
* Identify SCADA cyber vulnerabilities.
* Describe how an attacker may gain control of the SCADA system.
* Define vulnerability assessment and explain why it is important.
* Identify vulnerability assessment techniques and tools, such as CSET, Nessus, and other assessment tools.
* Explain the differences between vulnerability scanning and penetration testing.

**Required Reading:** Parfomak, Paul W. *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options.* CRS Report for Congress, RL33206. Updated September 12, 2008. Available from the Homeland Security Digital Library, https://www.hsdl.org/?abstract&did=235063.

**Team Activity**: Student teams continue to build a description of the operating environment for their sector-based organization, describing how they would use vulnerability scanning and/or penetration testing to evaluate threat potentials.

**Module 7: Risk Assessments**

**Description:** This module introduces risk assessment processes and the types of assessments available. Students download the Department of Homeland Security (DHS) CSET tool that was introduced in Lesson 6. They install it and use it to perform a Cybersecurity Framework Critical Infrastructure Risk Assessment.

**Module Objectives**:

* Identify the different risk assessment frameworks.
* Discuss Supply Chain Risk Management (SCRM) principles.
* Explain how regulatory requirements are used in determining additional items to review in a risk assessment.
* Demonstrate an understanding of the CSET tool risk assessment functions.
* Apply the CSET tool to an IT general risk assessment.
* Develop a report using CSET.
* Apply the standard available in the CSET tool to an IT general risk assessment.

**Hands-on Activity:** Students download the Department of Homeland Security (DHS) CSET tool, install it, and use it to perform a Cybersecurity Framework Critical Infrastructure Risk Assessment.

**Team Activity:** Student teams use the CSET tool to produce a risk assessment report for their sector-based organization.

**Module 8. Remediation**

**Description:** This module covers how to control risk to the network through appropriate remediation techniques. It introduces the concept of the Security Design Life Cycle (SDLC) and the importance of building security in at initiation, rather than “bolting” it on afterwards. In ICS and other SCADA systems, this may not be possible. Foundation guidelines and policies for controlling risk and personnel behavior will be addressed. An enumeration of network protection systems will be provided, including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

The module discusses the importance of digital signatures to providing device authentication, and how vulnerabilities specific to ICS systems relate to remediation techniques. Additionally, it covers common vulnerabilities found in ICS systems and techniques to identify vulnerabilities, as well as remediation techniques.

**Module Objectives**:

* Describe how risk management techniques control risk.
* Explain the concept of the Security Design Life Cycle (SDLC).
* List the types of security policies and how these relate to remediation.
* Describe how awareness and training can provide increased security.
* Identify remediation techniques in an ICS network, including routers, firewall technology, and tools for configuring firewalls and routers.
* Describe intrusion detection and prevention systems and web-filtering technologies.
* Explain the importance of digitally signed code for pushes of firmware and other updates to automated devices.
* Demonstrate the ability to evaluate and assess vulnerabilities in ICS networks.
* Explain and make recommendations for remediation strategies in an ICS network.
* Describe the hazards (do and don’ts) of the corporate network process vs. ICS network process.

**Hands-on Activity:** Students download and install a digital certificate.

**Team Activity:** Based on the risks that teams identified for their sector-based organization’s infrastructure in Module 7, student teams identify appropriate security controls to mitigate these risks.

**Module 9. Incident Response**

**Description:** Students learn about Incident Response (IR) strategies, including prevention and containment. They also learn how to create an Incident Response Plan.

**Module Objectives**:

* List some common types of incidents that may occur in SCADA/ICS systems.
* Identify the phases of an Incident Response (IR), as described in the NIST SP 800-61.
* Define incident containment and describe how it is applied to an incident.
* Discuss the IR reaction strategies unique to each category of incident.
* Explain the components of an Incident Response Plan.
* Identify the 14 response core capabilities covered in the National Response Framework.

**Required Reading**:

* Department of Homeland Security (DHS). *Presidential Policy Directive 8: National Preparedness (PPD-8).* March 30, 2011. Download from https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
* Federal Emergency Management Agency (FEMA), Department of Homeland Security (DHS). *National Response Framework.* Third Edition. June 2016. Download from https://www.fema.gov/media-library/assets/documents/117791.
* Federal Emergency Management Agency (FEMA), Department of Homeland Security (DHS). *National Incident Management System.* Download from https://www.fema.gov/media-library-data/1467113975990-09cb03e2669b06b91a9a25cc5f97bc46/NE\_DRAFT\_NIMS\_20160407.pdf.

**Hands-on Activity:** Students review one NIST case study, either the Olympic Pipeline Explosion or the Maroochy Water Services Incident. They indicate the response steps and describe what went wrong.

**Team Activity**: Teams select one of the risks from their risk assessment and create an Incident Response Plan for their sector-based organization.

**Module 10. Policy and Governance**

**Description:** This module covers policies and governance issues. Topics covered include federal Critical Infrastructure policies and legislation, information sharing of threats among agencies, public/private partnerships, and standards and regulations, as well as compliance. Issues relevant to specific sectors is discussed, such as intellectual property, and the roles of HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and PCI (DSS) are reviewed.

**Module Objectives**:

* Identify information-sharing strategies and initiatives as established by the Department of Homeland Security (DHS).
* Describe threat intelligence information sharing among public and private partners, including Information Sharing and Analysis Centers (ISACs).
* Explain the roles that DHS’s National Cybersecurity and Communications Integration Center (NCCIC) and National Infrastructure Coordinating Center (NICC) play in infrastructure protection.
* Describe issues relevant to specific critical infrastructure sectors, such as HIPAA and other regulations and laws.

**Required Reading:**

* Department of Homeland Security. *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience.* A PDF of this document can be downloaded from https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.
* ISAC Council. *The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection.* January 2009. PDF available online at http://www.isaccouncil.net/images/ISAC\_Role\_in\_CIP.pdf.
* Congressional Research Service (CRS). *Cybersecurity: Selected Legal Issues.* CRS Report for Congress 7-5700, R42409. April 17, 2013. Available for download in PDF and other digital formats from the Internet Archive at https://archive.org/details/208169CybersecuritySelectedLegalIssues-crs.
* Department of Homeland Security. “About the National Cybersecurity and Communications Integration Center.” Last Published Date: January 19, 2016. Online at https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.
* ThreatConnect. *Threat Intelligence Platforms: Everything You’ve Ever Wanted to Know But Didn’t Know to Ask.* E-book. Arlington, VA: ThreatConnect, 2015. Available for download from https://www.threatconnect.com/download-ebook/.

**Team Activity:** Student teams identify the policy and governance issues for their selected sectors.

**Module 11. Trends**

**Description:** This module discusses the future of cybersecurity: the Internet of Things (IoT) and how it creates an entirely new set of risks, and emerging technologies like drones, robots, and “wearables.” Increasingly, companies and organizations are exploring a more “active defense” approach to cybersecurity. Traditional incident response—the rapid deployment of a team to remediate breaches to a network, identify additional threats, and restore functionality—is still necessary but is no longer sufficient. The module gives an overview of how the connectedness of our cyber networks demands intelligence-driven tools and processes that equip leaders with an anticipatory edge.

**Module Objectives**:

* Identify emerging trends and demonstrate an understanding of emerging technologies.
* Understand the Internet of Things (IoT) and how it expands the cyber “attack surface.”
* Be able to make educated predictions of what the future might look like for the cybersecurity critical infrastructure framework.
* Discuss ethical issues that can arise in relation to new technology and new defense strategies.

**Required Reading:** The President’s National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on the Internet of Things.* Nov. 18, 2014. PDF file available for download at https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf.

**Hands-on Activity:** Individual students write concise reports on a recent trend in the sector they have been studying.

**Team Activity:** Student teams organize the materials on their sector and their fictitious organization into a final presentation to be shared with the class.

 **Module 12: Sector Report Outs**

**Description:** Each student team presents a summary of its case study project for the class. Team presentations should offer insights into what the students have learned from this course. Depending on the number of teams in the class, it may take more than one class period for all projects to be presented.

**Module Objectives**:

* Demonstrate the ability to communicate technical and business information in a presentation format.
* Demonstrate the ability to interact with peers and others.
* Demonstrate the professionalism and soft skills employers look for in an employee.

**Supplemental Materials & Resources**

**Books**

American Psychological Association. *Publication Manual of the American Psychological Association*. 16th edition. Washington, DC: American Psychological Association, 2009. Available from http://www.apastyle.org.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, 2nd Ed. Hoboken, NJ: Wiley Publishing, 2015. ISBM 978-1-118-81763-6. Information about this textbook can be found at http://www.wiley.com/WileyCDA/WileyTitle/productCd-111881763X.html. The book’s companion website is at http://www.wiley.com//legacy/wileychi/lewis/.

Miller, Stephen, and Clark, Richard H. *Framework for SCADA Cybersecurity.* Smashwords Edition, eBook ISBN 978-1310-30996-0. Available at https://www.smashwords.com/books/view/510004.

Parfomak, Paul W. *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options.* CRS Report for Congress, RL33206. Updated September 12, 2008. Available from the Homeland Security Digital Library, https://www.hsdl.org/?abstract&did=235063.

ThreatConnect. *Threat Intelligence Platforms: Everything You’ve Ever Wanted to Know But Didn’t Know to Ask.* E-book. Arlington, VA: ThreatConnect, 2015. Available for download from https://www.threatconnect.com/download-ebook/.

**Videos**

*Cyber War: Cybercrimes with Ben Hammersley.* BBC News, 2016. 6 episodes. Videos may be available through the Films on Demand service of Infobase (many college and university library systems subscribe): http://www.infobasepublishing.com/StreamingFODLanding.aspx.

**Government Resources**

ICS-CERT Virtual Learning Portal, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Department of Homeland Security. Among the resources available to registered users is the Secure Architecture Design graphic used in the Module 3 Hands-on Activity. Access at https://ics-cert-training.inl.gov/lms/.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Department of Homeland Security. Instructor-led and web-based training events on industrial control systems cybersecurity. Available at https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

**Online Training and Tools**

CSET risk assessment tool. The Cyber Security Evaluation Tool (CSET) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed by cybersecurity experts under the direction of the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The tool can be downloaded from this website: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET. A fact sheet on the CSET is available for download: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT\_FactSheet\_CSET\_S508C.pdf.

Oracle VM VirtualBox. This cross-platform virtualization software makes it possible to set up a virtual PC on a Mac so you can install and run CSET. VirtualBox can be downloaded from https://www.virtualbox.org/. Documentation in how to use VirtualBox is available here: https://www.virtualbox.org/wiki/End-user\_documentation.

SCADA Hacker’s Toolset. This webpage lists online resources and tools for control system security testing. The list is part of the website www.scadahacker.com, published by Joel Langill, the Director of Critical Infrastructure and SCADA representative for the Cyber Security Forum Initiative. URL: https://www.scadahacker.com/tools.html.

VMware Workstation. This application makes it possible to run multiple operating systems as virtual machines on a single PC. A free trial of the software can be obtained by clicking the “Get Free Trial” option under Product Resources on the following webpage: https://my.vmware.com/web/vmware/info?slug=desktop\_end\_user\_computing/vmware\_workstation/10\_0.