Lesson 9 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 9 TOPIC: INSIDER THREATS AND CYBERSECURITY AND SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) VULNERABILITIES

1. Lesson Goals/Objectives:

- Discuss the multi-dimensional, evolving nature of the "insider threat" to critical infrastructure.
- Examine the linkages between cybersecurity and CISR from an operational and security perspective.
- Identify and evaluate the challenges presented by information technology and SCADA systems vulnerabilities.
- Discuss the different approaches used to address malicious actor/cyber threats and secure the cyber components of critical infrastructure systems.
- Identify and evaluate the elements of an effective framework for enhancing CISR in the context of malicious cyber threats.

2. Discussion Topics:

- Characterize the threat to critical infrastructure assets and systems posed by malicious actors.
- What are the typical motivations of the various types of malicious actors that can disrupt our CI and harm our critical work force?
- How are malicious actor threats to CI identified and assessed? How do the SNRA and THIRA processes account for the malicious actor threat? Which types of events are most likely? The most consequential?
- What are the key elements of an effective approach to increase the security of the critical sectors in the context of malicious actor threats? What role does resilience play in mitigating threats from a malicious actor incident?
- How does the 2008 NIAC Report, *The Insider Threat to Critical Infrastructure*, characterize this type of threat? What are the major obstacles that complicate addressing of the insider threat?
- What are the principal threats and challenges of cybersecurity as they pertain to CISR? Is this a "real and present danger?" Why or why not?
- Discuss the major components of the U.S.'s *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* What are the strengths and weaknesses of the U.S. approach?
- What are the major elements of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity?* Does this

framework offer a useful approach in enabling the identification, assessment, and management of cyber threats? Why or why not.

- Who "owns" the cyber problem? On the government side? On the private sector side? How does each party communicate and coordinate with the other to jointly address cyber risk?
- How is cyber risk assessed and mitigated within and across the critical infrastructure sectors? How do we know when we are making a difference in this domain? How can risk reduction be measured?
- Is Federal regulation required to mitigate risk across all sectors subject to the cyber threat? If so, what would such a regime look like?
- How do Supervisory Control and Data Acquisition (SCADA) system concerns relate to the critical infrastructure sectors? How are the various critical infrastructure sectors dealing with the evolving threat to SCADA systems?
- Discuss the major components of the USCERT *Cross Sector Roadmap for Cyber-Security of Control Systems.* Does the approach outlined therein lay out a viable path forward in addressing cyber threats to SCADA systems?
- What are the core elements of an effective cybersecurity strategy? How does the concept of "defense-in-depth" apply to the world of cybersecurity?

3. In-class Exercise. The class will be broken down into two teams. Each team will discuss and catalog the "pros and cons" of the *Framework for Improving Critical Infrastructure Cybersecurity* issued by the NIST, with an eye toward its applicability to the identification, assessment, and management of cyber threats within a specific critical infrastructure sector assigned by the instructor. Learners should also be able to discuss the sector-specific cyber security roadmaps available on line.

4. Required Reading:

Collins and Baggett, Chapter 10.

Lewis, Chapters 8, 9 & 10.

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, http://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

US-CERT, *Cross-Sector Roadmap for Cybersecurity of Control Systems*, September

2011, https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/Cross-Sector_Roadmap_9-30.pdf

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Sam Powers, *The Threat of Cyberterrorism to Critical Infrastructures*, 2013, http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/

Industrial Control Systems-Cyber Emergency response Team (ICS-CERT), *Cyber Threat Source Descriptions*, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

Georgia Tech Information Security Center, Security Summit, *Emerging Cyber Threats Report, 2013*, https://www.gtisc.gatech.edu/pdf/Threats_Report_2013.pdf

National Infrastructure Advisory Council, *Convergence of Physical and Cyber Technologies and Related Security Management Challenges*, 2007, http://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf

North American Electricity Reliability Corporation, *High-Impact Low-Frequency Event Risk to the North American Bulk Power System*, 2010, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf (Physical-Cyber Threat Section)

U.S. Government Accountability Office, *Cyber Security: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*, 2010, http://www.gao.gov/new.items/d10834t.pdf

Peter Allor, *Understanding and Defending Against Foreign Cyber Threats*, (2007), http://www.homelandsecurity.org/journal/Default.aspx?oid=165&ocat=1.

U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Needs to Better Address its Cyber Security Responsibilities*, 2008, http://www.gao.gov/new.items/d081157t.pdf.

Mariana Hentea, *Improving Security for SCADA Control Systems*, 2008, http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf.

U.S. Government Accountability Office, *Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*, 2010, http://www.gao.gov/new.items/d10834t.pdf.

4. Additional Recommended Reading:

Stouffer, Falco and Kent. *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrialized Control Systems Security.* 2006. http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20(2007).pdf.

Jason Stamp, Phil Campbell, Jennifer DePoy, John Dillinger, and William Young, *Sustainable Security for Infrastructure SCADA*, 2003, http://energy.sandia.gov/wp/wp-content/gallery/uploads/SustainableSecurity.pdf.

David Watts, *Security and Vulnerability in Electric Power Systems*, 2003, http://web.ing.puc.cl/~power/paperspdf/WattsSecurity.pdf

U.S. Government Accountability Office, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, (March 2004), http://www.gao.gov/new.items/d04354.pdf.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 9(7), January 2011, http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_January2011__Cybersecurity.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 9: Insider Threats, Cybersecurity and Supervisory Control and Data Acquisition (SCADA) Vulnerabilities

Lesson 9 Outcomes/Objectives

- Discuss the multi-dimensional, evolving nature of the “insider threat” to critical infrastructure.
- Examine the linkages between cybersecurity and CISR from an operational and security perspective.
- Identify and evaluate the challenges presented by information technology and SCADA systems vulnerabilities.
- Discuss the different approaches used to address malicious actor/cyber threats and secure the cyber components of critical infrastructure systems.
- Identify and evaluate the elements of an effective framework for enhancing CISR in the context of malicious cyber threats.

CI Threat-related EEIs

- Identify and characterize threat or hazard actor/vector
- Identify how the threat/hazard would be recognized or manifest itself
- Identify target/potential communities of impact
- Identify expanse/distribution
- Establish timing parameters/likelihood of recurrence
- Identify vulnerabilities likely to be exploited by threat/hazard
- Identify likely impacts
- Identify potential connections to other threats/hazards

Types of Malicious Actor Threats to CI

- **Bad Actor**
  - Foreign intelligence entities (Nation-states)
  - Transnational terrorists
  - Domestic terrorists/homegrown violent extremists (HVEs)
  - International/domestic criminal organizations (financial motivations)
  - Malicious insider (individual(s) affiliated with any of the above, disaffected employee(s), mentally disturbed employee(s))

- **Bad Act** (Target = people, physical assets, data, data systems)
  - Inflict physical harm on people or damage physical facilities, critical systems, equipment, etc.
  - Data Breaches, including identity or intellectual property theft
  - Industrial Sabotage
  - Gain control of a critical cyber function to disrupt services or cause harm to people and property

The Insider Threat

- *Definition: "one or more individuals with the access and/or inside knowledge of a company, organization or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products or facilities with the intent to cause harm."* (Includes employees, unescorted vendors, consultants and contractors)

- Rapidly advancing technology and network risks are combining with growing globalization of workforces, supply chains and service providers to produce new risks.

- Virtual work environments are replacing static workplace boundaries, pushing toward decentralization and expanding a company's attack surface.

- As technology has become more portable, so have the tools available to malicious insiders.
  - Malicious code or hacking tools can be accessed via networks or brought into the environment on miniaturized computing or storage devices. Exploit tools are increasingly stealthy, elevating the difficulty of detection and remediation.

- New business models and software tools now allow a single individual to manage many platforms that can be located around the globe.

The Insider Threat (Cont.)

- Lack of an appropriate awareness of the threat—insiders are typically discovered only after they have already committed a malicious act.
- Varying levels of access to tools and information to conduct adequate background screens of potential employees.
- Globalization has expanded inside access and knowledge to new populations that are less verifiable than existing workers.
  - Variation among international legal environments is an acute challenge, with employee screening being the most obvious.
  - Cultural norms and legal protections for personal privacy on IT systems vary significantly between countries.
- Need for improved cross-platform insider threat data correlation tools to assist in identifying anomalies/behavior patterns across IT and physical access systems.
- “Institutional” issues:
  - unquestioned and unverified trust of employees after granting employment;
  - poor operator-workforce union relationships;
  - employee expectations of rights and privileges versus obligations; and
  - prevailing attitudes about management involvement in workers’ personal lives.

Industrial Control Systems

- Today's ICS are highly network-based and use common communications technologies (Internet, public-switched telephone, cable or wireless networks) and protocols.
- Increased adoption of COTS, providing greater levels of interoperability required among today's modern infrastructures.
- Potential for system access resulting from greater interoperability exposes network assets to infiltration and subsequent manipulation of sensitive ops.
- Increasingly sophisticated cyber attack tools can exploit vulnerabilities in commercial off-the-shelf system components, telecommunication methods and common operating systems found in modern ICS.
- Emergent issues: increasing connectivity, proliferation of access points, escalating system complexity, greater interdependencies, increased outsourcing/reliance on foreign products and wider use of common operating systems and platforms.
- ICS security policies and practices are often poorly implemented.

Industrial Control Systems (Cont.)

- **Major Goals of the Cross-sector ICS Roadmap**
  - Measure and assess security posture *(through use of* supporting tool and methodology provided).
  - Develop and integrate protective measures.
  - Detect intrusion and implement response strategies.
  - Development and employment of tailored performance metrics.

NIST Cybersecurity Framework

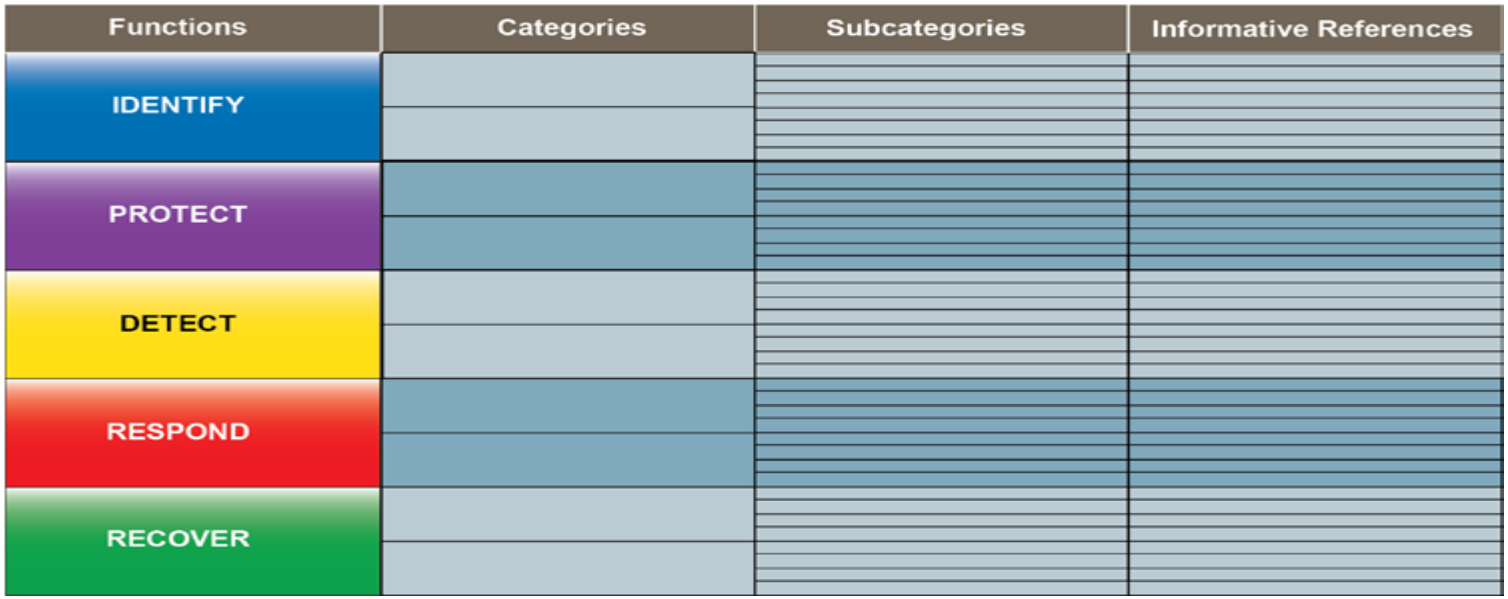
- EO 13636 called for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks.

- Framework provides common taxonomy and mechanism for organizations to:
  - Describe their current cybersecurity posture;
  - Describe their target state for cybersecurity;
  - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
  - Assess progress toward the target state; and
  - Communicate among internal and external stakeholders about cybersecurity risk.

- Focuses on using business drivers to guide cybersecurity activities and consider cyber risks as part of an organization's risk management processes.

NIST Cybersecurity Framework (Cont.)

- Framework consists of 3 parts: Core, Profile and Implementation Tiers.
  - Core: a set of cybersecurity activities, outcomes and informative references that are common across CI sectors, providing the detailed guidance for developing individual organizational Profiles.
    - Includes 5 concurrent/continuous Functions—Identify, Protect, Detect, Respond, Recover.
    - Identifies underlying key Categories/Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines and practices for each Subcategory.



NIST Cybersecurity Framework (Cont.)

- Profiles: help an organization align its cybersecurity activities with its business requirements, risk tolerances and resources based on business needs selected from the Framework Categories and Subcategories.
  - Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile with a “Target” Profile
- Tiers: provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.
  - Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4).

How Can the NIST Framework be Used?

- Comparison of an organization's current cybersecurity activities with target capabilities derived through application of the Framework.
- Assessment of how identified risks are managed, and how an organization compares to existing cybersecurity standards, guidelines and practices.
- Address specific risks, and corresponding target performance enhancements and investments.
- Measurement of performance and efficacy of investments over time through a repeatable process.
- Inform supply chain partner cybersecurity requirements.

Lesson 9 In-class Activity

- The class will be broken down into two teams. Each team will discuss and catalog the “pros and cons” of the *Framework for Improving Critical Infrastructure Cybersecurity* issued by the NIST, with an eye toward its applicability to the identification, assessment, and management of cyber threats within a specific critical infrastructure sector assigned by the instructor. Learners should also be able to discuss the sector-specific cyber security roadmaps available on line.

Discussion Questions

- Characterize the threat to critical infrastructure assets and systems posed by malicious insiders. How do such threats potentially impact CI ops and services?

- What are the typical motivations of the various types of insiders that can disrupt our CI and harm our critical work force?

- How are insider threats to CI identified and assessed? How do the SNRA and THIRA processes account for the malicious actor threat? Which types of events are most likely? The most consequential?

- What are the key elements of an effective approach to increase the security of the critical sectors in the context of malicious actor threats? What role does resilience play in mitigating threats from a malicious actor incident?

- How does the 2008 NIAC Report, *The Insider Threat to Critical Infrastructure*, characterize this type of threat? What are the major obstacles that complicate addressing of the insider threat?

Discussion Questions (cont.)

- What are the principal threats and challenges associated with the cyber domain as they pertain to CISR?
- Who “owns” the cyber problem? On the government side? On the private sector side? How are cyber threats jointly assessed and mitigated?
- Discuss the major components of the U.S.’s *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* What are the strengths and weaknesses of the U.S. approach?
- How is cyber risk assessed and mitigated within and across the critical infrastructure sectors? How do we know when we are making a difference in this domain?
- How are the various CI sectors dealing with threats to SCADA systems?
- Discuss the major components of the USCERT *Cross Sector Roadmap for Cyber-Security of Control Systems.* Does the approach outlined therein lay out a viable path forward in addressing cyber threats to SCADA systems?

Discussion Questions (cont.)

- What are the major elements of the NIST *Framework for Improving Critical Infrastructure Cybersecurity?* Does this framework offer a useful approach in enabling the identification, assessment, and management of cyber threats?

- What are the core elements of an effective cybersecurity strategy? How does the concept of “defense-in-depth” apply to the world of cybersecurity? The PPD-8 capability development process?

- Is Federal regulation required to mitigate risk across all sectors subject to the cyber threat? If so, what would such a regime look like?

- Discuss the nexus between the physical and cyber insider threat. How are insider threat defense mechanisms similar/different given the cyber/physical characteristics of each? How might a layered approach to security be arranged to defend against both?