**Certificate Program in Critical Infrastructure Security and Resilience**

**Course Number: XXXX**

**Course: Critical Infrastructure Security, Resilience, and Cybersecurity**

**University of XXXXXX Fall/Spring Semester 20XX**

**NAME OF SCHOOL: DEPARTMENT: PROGRAM: PROFESSOR:**

Telephone Number:

Office Location: Office Hours: Email:

Website:

**COURSE DESCRIPTION/OVERVIEW:**

Our economic vitality and national security depend today on a vast array of complex networks, systems, services, and resources. Within this vast interdependent and interconnected world, information systems are an increasingly essential component of our government, economy, social structure, and critical infrastructure sectors. Without these systems, we would not be able to communicate, travel, enjoy safe drinking water, provide electricity to homes and businesses, manage the economy, obtain government services, or provide for the defense of the Nation. The interdependent world in which we live is also characterized by a host of new, complex threats, vulnerabilities, and increased risk.

This 15-lesson graduate level course provides an introduction to the policy, strategy, and operational environment of cyberspace in the context of the critical infrastructure security and resilience mission area. The course includes a discussion of the cybersecurity challenges presented by the 21st century risk environment, as well as the opportunities and challenges associated with the following: cyber risk analysis and prioritization; risk mitigation and management; performance measurement; government-private cybersecurity partnerships and information-sharing; attack alert and response; incident management; and addressing future cyber risks.

This is a multi-faceted course that will expose participants to complex intergovernmental and government-private sector cybersecurity policy-making; risk analysis and management; future planning; and national incident management. The course is designed to promote subject-matter understanding, critical analysis, and insight into complex policy and operational issues. It also includes a practical examination of stakeholder interaction and key subject-matter areas through a series of in-class exercises, an interactive tabletop exercise, research paper, and oral presentation. The course promotes a holistic understanding of various approaches to cybersecurity, applicable to the critical infrastructure sectors identified in the National Infrastructure Protection Plan (NIPP), as well as information infrastructures and relationships which cross national borders or are inherently international.

This course does not provide a technical or tactical focus on information, operations, or communications security. It is not designed for computer technicians or systems analysts with an in-depth knowledge of the cyber world. Rather, the course is targeted at the strategic level of understanding, with material regarding technical cyber systems information and concepts provided as required to serve as a background for broader policy and strategic discussions.

C**REDITS CONFERRED:** 3

**PREREQUISITES:**

• Course Number XXXX: Foundations of Critical Infrastructure Security and Resilience

• Course Number XXXX: Partnering and Information Sharing for Critical Infrastructure

Security and Resilience

• Course Number XXXX: Assessing and Managing Risk to Critical Infrastructure Systems

**LEARNER OUTCOMES/OBJECTIVES**

This course is designed to enable learners to:

**1.** Assess and apply key concepts as they relate to various aspects of cybersecurity and critical infrastructure security and resilience.

**2.** Explain the linkages between the cybersecurity and critical infrastructure security and resilience mission areas and how each of these systems influences the other.

**3.** Understand the fundamental operating concepts, characteristics, hardware and software structure, and governance elements of the Internet.

**4.** Explain how cybersecurity evolved as a core homeland security policy area.

**5.** Recognize and assess risk associated with cyber components of critical infrastructure sectors:

• Threats: terrorism, natural disasters and other naturally occurring phenomena, manmade events, technological failure, and other emergencies

• Vulnerabilities (facility, node, system, and sector level)

• Consequences (public health and safety, economic loss/disruption, mission disruption, continuity of government and essential services, etc.)

• Dependencies/interdependencies

• Informing executive and managerial decision-making that can reduce risk and increase resilience for the Nation

**6.** Apply the various strategic approaches regarding cyber risk management and performance measurement to the pertinent critical infrastructure sectors.

**7.** Describe the requirements and implications of the authorities, roles, responsibilities, and capacities of key cybersecurity public and private sector stakeholders:

• Federal, State, local, tribal, territorial, regional, and private sector

• International

• Private sector issues and concerns

• Regulations, incentives, and motivations

**8.** Obtain working knowledge of the current cybersecurity partnership frameworks, information sharing processes and systems, and coordination/collaboration challenges:

• Federal, State, local, tribal, territorial, regional, private sector collaboration, coordination, and communication

• International collaboration, coordination, and communication

**9.** Explain how the national-level cyber incident management framework and coordination

structure operate across the spectrum of prevention, protection, mitigation, response, and recovery.

**10.** Assess the complexities of cybersecurity program management in a dynamic risk and future operating environment:

• Developing sector-specific, jurisdictionally-based, or regionally-focused cybersecurity goals, objectives, risk mitigation approaches, and plans

• Designing and applying continuous feedback mechanisms to measure cybersecurity program performance

• Designing and implementing cybersecurity awareness, education, and training programs

• Planning for the future risk and cyber operating environments

**DELIVERY METHOD:**

Learners will develop an understanding of the subject-matter of the course and meet course objectives through a combination of assigned readings, lectures, group discussion, in-class exercises, written projects, in-class oral presentation, and a cyber incident management exercise. Learning will include a mix of independent study and group discussion and collaboration.

The assigned course readings include a variety of resources, such as government documents (legislation, executive orders, policies, plans, and strategies), academic readings (textbooks, journal articles, research studies and reports), and third-party reviews (U.S. Government Accountability Office (GAO) reports, Congressional Research Service (CRS) reports, etc.). Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases, particularly the external reviews, and from multiple perspectives. The instructor will facilitate the discussion by asking different levels of questioning (factual, analytical, and application of the material) to evaluate the depth of the learner’s comprehension of the content.

The course is designed to be delivered in a typical 15-week semester format (approximately 40-45 hours). The course can be easily adapted to be delivered in alternative formats to include

half-semesters (7-8) weeks, one week, and through distance learning.

**GENERAL COURSE REQUIREMENTS:**

**1.** Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.

**2.** It is expected that assignments will be turned in on time (the beginning of the class in which they are due). However, it is recognized that learners occasionally have serious problems that prevent work completion. If such a dilemma arises, please speak to the professor in a timely fashion.

**3.** The completion of all readings assigned for the course is assumed. Since the class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class.

**4.** According to university policy, all cell phones should be turned off before class begins.

**GRADING:**

Learners will be assessed on their post course knowledge through written research and practical exercises/projects. Learners will be required to achieve a passing grade in order to receive credit for completing the course.

|  |  |
| --- | --- |
| Class Participation | 35% |
| Cyber Incident Management Paper & | 25 % |
| Exercise Participation |  |
| Research Paper | 30% |
| In-class Research Paper Presentation | 10 % |
| **Total** | **100 %** |

**RESEARCH PAPER AND IN-CLASS PRESENTATION**

**1. Research Paper (30%):**

**Option 1**: The learner will prepare a 12-15 page (double-spaced) research paper on a relevant topic of interest in the area of cybersecurity as applied to the critical infrastructure security and resilience mission area. The paper should clearly state a hypothesis and propose a solution to a known issue or problem. The paper should strive to support the hypothesis or solution recommended with authoritative reports, articles, interviews, or other data. The paper should be organized using the following format: problem statement, background (include key players, authorities, resources, etc.), discussion (presentation of the issue and alternative solutions, identifying pros and cons for each alternative), and recommendations (including rationale behind their selection). Footnotes and citations should be included on a separate sheet of paper in the proper format for review. The paper should focus on the benefits, drawbacks, and obstacles to the practical application of the proposed solution. The recommendations section should clearly describe the rationale for the solution of choice.

**Option 2**: In lieu of the above, learners may elect to develop a comprehensive written cyber risk assessment and cyber risk management strategy for a particular critical infrastructure sector,

sub-sector, or system. As a first step, learners will provide a detailed analysis of the cyber components of the infrastructure sector, sub-sector, or system itself, consisting of the following elements: cyber component definition/description; illustrative block diagram; and summary of

stakeholders and their perspectives pertaining to the cyber components of the sector, sub-sector, or system. Next, learners will use their knowledge of the infrastructure sector, sub-sector, or system selected to comprehensively identify cyber-related vulnerabilities, describe the types of threats that could exploit these vulnerabilities, and estimate how compromising the sector, sub-sector, or system from a cyber perspective will adversely affect the interests of one or more stakeholders. Learners will then identify various approaches/options for mitigating identified vulnerabilities and evaluate them in terms of their costs and benefits and ability to reduce or manage risk. Finally, learners will define a set of performance metrics that can be used to measure the effectiveness and efficiency of the cyber risk management approaches selected over time.

The research paper is due at the beginning of class in **Lesson 15**. Prior instructor approval of the topic for either of the two research paper options is required. Learners must submit a

one-paragraph written description of their proposed topic to the instructor for approval no later than the beginning of class in **Lesson 4**. All data used for this assignment will be properly cited; when data is unavailable, all assumptions with justification will be appropriately articulated.

**2. In-Class Research Paper Presentation (10%):**

Each learner will present his/her research paper topic (no more than 15-20 minutes in length) to the class during **Lessons 14-15**. Following each presentation, learners will have 5 additional minutes allotted to field questions from fellow learners. The presentation format will mirror that of the research paper as detailed above for either option.

**3. Cyber Incident Management Exercise (25%):**

Learners will participate in a role-based, interactive tabletop exercise simulating a complex, malicious attack on the cyber components of multiple critical infrastructure sectors. The outline for this exercise is provided in **Attachment 1**. Each learner will be assigned a role as a key public or private sector official with attendant cybersecurity and critical infrastructure responsibilities. The exercise will include emerging threat, operational response, and post-incident recovery phases. In preparation for the exercise, each participant will develop a short 3-5 page paper in talking point format delineating his/her assigned role-based responsibilities during each phase of exercise play. Learners will be graded based on their point paper submission as well as their participation during the exercise. **This paper will be submitted by the beginning of class on the day of the exercise.**

**INCORPORATION OF FEEDBACK:**

Multiple opportunities for constructive feedback between the instructor and learners will be provided over the period of the course. These feedback channels may take the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to provide written mid-term feedback at the end of class on Lesson 6 and at the end of the course. On-line feedback to the instructor is also encouraged at any time throughout the course. Finally, the instructor will provide written feedback on all oral and written assignments that form part of this course. Ongoing dialogue with the instructor regarding research paper development, oral presentation preparation, and other in-class assignments is highly encouraged.

**COURSE TEXTBOOKS**

The following are the primary textbooks for this course. These textbooks will be supplemented by additional readings accessible on-line, with website addresses provided in the lesson description section that follows.

John W. Rittinghouse and William M. Hancock, *Cybersecurity Operations Handbook*, Elsevier Digital Press, (2003), ISBN: 1-55558-306-7.

Linda Volonino and Stephen R. Robinson, *Principles and Practice of Information Security*, Pearson Prentice Hall, (2004), ISBN: 0-13-184027-4.

Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, (2010), ISBN: 978-160650-197-9.

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (eds), *Cyberpower and National* *Security*, National Defense University Press, (2009), ISBN: 978-1-59797-423-3.

**ADDITIONAL RESOURCES:**

Black Hat: [http://www.blackhat.com/.](http://www.blackhat.com/)

The Center for Infrastructure Protection and Homeland Security, *The CIP Report*,

Cybersecurity: http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013

/06/CIPHS\_TheCIPReport\_January2011\_\_Cybersecurity.pdf

The Center for Infrastructure Protection and Homeland Security, *The CIP Report*,

Cybersecurity: <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_April2012_Cybersecurity.pdf>

DEF CON: [http://www.defcon.org/.](http://www.defcon.org/)

Georgetown University’s Institute for Law, Science, and Global Security Cyber

Project: [http://lsgs.georgetown.edu/programs/CyberProject/.](http://lsgs.georgetown.edu/programs/CyberProject/)

George Washington University’s Homeland Security Policy

Institute: [http://www.gwumc.edu/hspi/policy/issue\_cyber.cfm (](http://www.gwumc.edu/hspi/policy/issue_cyber.cfm)frequent events).

IEEE: [http://www.ieee.org/index.html.](http://www.ieee.org/index.html)

International Telecommunications Union, Cybersecurity: [http://www.itu.int/cybersecurity/.](http://www.itu.int/cybersecurity/)

International Telecommunications Development Sector, Cybersecurity: [http://www.itu.int/ITU-D/cyb/cybersecurity/.](http://www.itu.int/ITU-D/cyb/cybersecurity/)

The Internet Engineering Task Force (IETF): [http://www.ietf.org/.](http://www.ietf.org/)

NATO Cooperative Cyber Defence Centre of Excellence: [http://www.ccdcoe.org/.](http://www.ccdcoe.org/)

RSA Conference: [http://www.rsaconference.com.](http://www.rsaconference.com/)

U.S. Department of Homeland Security: Office of Cybersecurity and Communications: [www.dhs.gov/office-cybersecurity-and-communications](file:///C:\Users\ckramer5\Desktop\www.dhs.gov\office-cybersecurity-and-communications)

U.S. Department of Homeland Security: U.S. Computer Emergency Readiness Team http://www.us-cert.gov/

Workshop on Economics of Information Security (WEIS):

* WEIS 2011: <http://weis2011.econinfosec.org/index.html>
* WEIS 2013: <http://weis2013.econinfosec.org/>
* WEIS 2014: <http://weis2014.econinfosec.org/>

**Blogs:**

[http://www.homelandsecuritynewswire.com/topics/cybersecurity.](http://www.homelandsecuritynewswire.com/topics/cybersecurity) [http://www.nextgov.com/cybersecurity/?oref=ng-nav.](http://www.nextgov.com/cybersecurity/?oref=ng-nav)

**COURSE OUTLINE**

**LESSON 1 TOPIC: INTRODUCTION TO CYBER SYSTEMS AND CYBERSECURITY CONCEPTS**

**1. Lesson Goals/Objectives:**

• Discuss general/specific course requirements, instructional methodology, evaluation criteria, and feedback processes.

• Explain the integrated role that cybersecurity plays in regard to critical infrastructure, our national economy, and national security.

• Identify and discuss the fundamental operating concepts, characteristics, hardware and software structure, and governance elements of the Internet.

• Explain the role that access control plays in cybersecurity, and be able to discuss the three pillars of access control: security policy, accountability, and assurance.

**2. Discussion Topics:**

• What are the definitions of cyber infrastructure, information assurance, information operations, and cybersecurity? How are they alike and how are they different?

• What are the core structural elements of cyberspace? How do they interact?

• What is an information infrastructure? What are the different components that typically comprise an information infrastructure?

• What are the core elements of an effective cybersecurity strategy?

• How does the NIPP address cybersecurity issues?

• What roles do the NICC and the NCCIC play in the national cybersecurity policy?

• Why is cybersecurity one of the most challenging global issues we face in regards to our economy and national security?

• What are the basic components of the Internet and its associated technologies? How does information transit the Internet?

• Why is it important to understand the basic components of Internet technology when working in or studying the cybersecurity field?

• How does the concept of “defense in depth” apply to the world of cybersecurity?

• What role does access control play in cybersecurity? What are the principal elements of access control and how are they linked?

**3. Required Reading:**

John W. Rittinghouse and William M. Hancock, *Cybersecurity Operations Handbook*, Elsevier Digital Press, (2003), Chapters 2 and 3.

Linda Volonino and Stephen R. Robinson, *Principles and Practice of Information Security*, Pearson Prentice Hall, (2004), Chapter 1.

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (eds), *Cyberpower and National*

*Security*, National Defense University Press, (2009), Chapters 1, 2 and 4.

U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 1-13,

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

Peter Sommer and Ian Brown, *Reducing Systemic Cyber Security Risk,* Organization for Economic

Cooperation and Development (OECD) Project on Future Global Shock, (January 14, 2011).

Tarek Saadewi and Louis Jordan, Jr., (eds), *Cyber Infrastructure Protection*, U.S. Army War College, (May 2011), Chapter 3.

Warriors of the Net Internet video, [http://www.warriorsofthe.net/index.html.](http://www.warriorsofthe.net/index.html)

**LESSON 2: THE EVOLUTION OF CYBERSECURITY POLICY IN THE UNITED STATES**

**1. Lesson Goals/Objectives:**

• Analyze the evolution of and nexus between cybersecurity and critical infrastructure security and resilience as national policy focus areas.

• Identify and discuss the major elements of the various statutes, Presidential policies, strategies, and other official government documents related to the cybersecurity mission area.

• Describe how our national approach to cybersecurity has evolved based upon new authorities and technologies, and has changed as a function of the risk environment over time.

**2. Discussion Topics:**

• How has the U.S. government’s approach to cybersecurity evolved in the past 15 years?

• What are the general principles typically associated with cybersecurity in the U.S. context?

How are these woven into strategy and policy at the national level?

• What are the strengths and weaknesses of the various Presidential policies focused on cybersecurity?

• Has our national approach toward cybersecurity done enough to extend cyber protections into the critical infrastructure sectors?

• Are current U.S. government and private sector cybersecurity programs designed to keep pace with fast changing, quick growth technology?

• How has the Nation’s policy structure and approaches to cybersecurity changed over time with regard to specific cyber threats and vulnerabilities?

• What progress have we made in implementing the various recommendations contained in the 2003 National Strategy to Secure Cyberspace? What have been the major impediments to progress?

• How do the White House’s 2009 Cyber Security Review Report, 2010 Comprehensive National Cyber Security Initiative, 2011 Cyber Legislative Proposal, and 2013 Executive Order address the cyber problem? Do they represent an effective collective approach? Why or why not?

• How do the 2010 National Security Strategy and 2014 Quadrennial Homeland Security

Review address cybersecurity?

• How does the U.S. Congress view the cybersecurity mission area? Will new cybersecurity legislation clarify or complicate this mission space?

**3. Required Reading:**

Rita Tehan, *Cybersecurity: Authoritative Reports and Resources, by Topic*, Congressional Research Service, pp. 12-23, (May 2, 2014), <http://nationalaglawcenter.org/wp-content/uploads/assets/crs/R42507.pdf> .

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (eds), *Cyberpower and National*

*Security*, National Defense University Press, (2009), Chapters 23 and 24.

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.](http://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

The Comprehensive National Cybersecurity Initiative, (2010), [http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.](http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)

U.S. Department of Homeland Security, *Quadrennial Homeland Security Review,*

(2014),  [http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf.](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf)

The White House, *National Security Strategy*, (May 2010), [http://www.whitehouse.gov/sites/default/files/rss\_viewer/national\_security\_strategy.pdf.](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf)

White House Cybersecurity Legislative Proposal,

(2011): <http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>

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

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 12, 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

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

**4. Recommended Reading:**

National Strategy for Trusted Identities in Cyberspace,

(2011), [http://www.whitehouse.gov/sites/default/files/rss\_viewer/NSTICstrategy\_041511.pdf.](http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf)

*The Journal of National Security Law and Policy*, [http://www.jnslp.com/topics/cybersecurity/.](http://www.jnslp.com/topics/cybersecurity/)

*The Harvard National Security Journal*, [http://harvardnsj.org/?s=cyber.](http://harvardnsj.org/?s=cyber)

**LESSON 3 TOPIC: UNDERSTANDING AND ASSESSING CYBER RISK**

**1. Lesson Goals/Objectives:**

• Ascertain the major elements of cyber risk in the context of critical infrastructure security and resilience and evaluate how they impact real-world operations.

• Describe how the evolving nature of the cyber threat and threat actors affects the realm of critical infrastructure security and resilience.

• Explain how critical infrastructure dependencies, interdependencies, and supply chain issues impact and are impacted by cyber risk.

**2. Discussion Topics:**

• Who is responsible for managing risk in the cyber domain?

* What are the major elements of the National Institute of Standards and Technology framework for the assessment of cyber risk? Does this framework offer a useful approach in bounding cyber risk assessment and management?

• How are the major elements of cyber risk determined/assessed?

• How do we define the term “threat” as it relates to the cyber domain? What are some examples?

• How do we apply the concept of likelihood determination to the cyber domain?

• How has the cyber threat to our critical infrastructure and related vulnerabilities evolved over time?

• Have technological advances in the information technology world made us more vulnerable? Why or why not?

• Does the Nation’s critical infrastructure represent preferred targets for malicious cyber actors? Who are these actors?

• What are the various approaches used by the different cyber threat actors?

• How do we define the term “vulnerability” as it relates to cyber? What are some examples?

• How is the consequence component of cyber risk defined and measured?

• How does the issue of critical infrastructure dependencies/interdependencies and interdependent supply chains complicate the cyber risk assessment process? How do we measure these dependencies and interdependencies?

• What is meant by the term “vulnerability assessment?” “Penetration testing?” “Audits?”

• How are audits used to help mature and sustain an organization’s security program?

• What are the major issues highlighted in the DHS Information Technology Sector Risk

Assessment?

**3. Required Reading:**

John W. Rittinghouse and William M. Hancock, *Cybersecurity Operations Handbook*, Elsevier Digital Press, (2003), Chapters 2, 3 and 14.

Linda Volonino and Stephen R. Robinson, *Principles and Practice of Information Security*, Pearson Prentice Hall, (2004), Chapter 3.

Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information* *Technology Systems*, National Institute of Standards and Technologies, Special Publication, 800-30, (July 2002), Chapters 2 and 3.

Steven Rinaldi, James Peerenboom, and Terrence K. Kelly, *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, (2004), [http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.](http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf)

National Defense University, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age*, (2008), [http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476034&Location=U2&doc=GetTRD](http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476034&Location=U2&doc=GetTRDoc.pdf)

[oc.pdf.](http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476034&Location=U2&doc=GetTRDoc.pdf)

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (eds), *Cyberpower and National*

*Security*, National Defense University Press, (2009), Chapters 6, 18, 19 and 20.

Georgia Tech Information Security Center, Security Summit 2011, *Emerging Cyber Threats Report* *2012*, <http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf>.

Tarek Saadewi and Louis Jordan, Jr. (eds), *Cyber Infrastructure Protection,* U.S. Army War College, (May 2011), Chapter 10.

U.S. Department of Homeland Security, “Information Technology Sector Risk

Assessment,” [http://www.dhs.gov/xlibrary/assets/nipp\_it\_baseline\_risk\_assessment.pdf.](http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf)

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

**4. Recommended Reading**:

The National Institute of Standards and Technology, *NIST Finalizes Initial Set of Smart Grid*

*Cyber Security Guidelines*, (September 2, 2010), [http://www.nist.gov/public\_affairs/releases/nist-finalizes-initial-set-of-smart-grid-cyber-security-guidelines.cfm.](http://www.nist.gov/public_affairs/releases/nist-finalizes-initial-set-of-smart-grid-cyber-security-guidelines.cfm)

The National Institute of Standards and Technology, *Revision of SP 800-53 Addresses Current*

*Cybersecurity Threats, Adds Privacy Controls*, (February 28, 2012), [http://www.nist.gov/itl/csd/sp800-022812.cfm.](http://www.nist.gov/itl/csd/sp800-022812.cfm)

**LESSON 4 TOPIC: DIFFERENT APPROACHES TO MANAGING CYBER RISK**

**1. Lesson Goals/Objectives:**

• Describe the elements of an effective cyber risk management framework and evaluate the various technical approaches designed to enable each.

• Describe the requirements of an effective cyber deterrence strategy.

• Evaluate the relationship between risk management and policy in the cybersecurity arena.

**2. Discussion Topics:**

• What are the basic elements of a cyber risk management framework? Is there a baseline “best practice” approach?

• What are some of the major technical approaches used to manage cyber risk?

• How does the IT SSP address the issue of cyber risk management? What are the principal challenges to this approach? How is performance measured over time?

• What are the specific steps to mitigate sector risk as discussed in the IT SSP?

• Can cyber attacks be effectively deterred?

• Compare and contrast market-based and regulatory approaches to cybersecurity.

• What are the major public policy issues associated with managing cyber risk? How do these policies impact risk management in the cyber arena, and vice versa?

• How does the issue of Internet governance affect the management of cyber risk?

• What are the major elements of the DHS Cyber Risk Assessment and Management Methodology? Is this product useful in creating an understanding of national level cyber risk and cyber-related dependencies/interdependencies across sectors?

**3. Required Reading:**

Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information*

*Technology Systems*, National Institute of Standards and Technologies, Special Publication

800-30, (July 2002), Chapters 4 and 5.

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (eds), *Cyberpower and National*

*Security*, National Defense University Press, (2009), Chapters 5, 7, 13, and 21.

Information Technology Sector Specific Plan, Chapters 2-6, <http://www.dhs.gov/information-technology-sector>

Georgia Tech Information Security Center, Security Summit 2011, *Emerging Cyber Threats Report* *2012*, <http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf>.

**LESSON 5 TOPIC: MANAGING RISK TO INDUSTRIAL CONTROL SYSTEMS (ICS)**

**1. Lesson Goals/Objectives:**

• Identify the common functions performed by SCADA/ICS within the critical infrastructure sectors.

• Evaluate the convergence and the differences between ICS/SCADA and information technology.

• Describe the nature of the cyber threat and resulting challenges and security trends in relation to ICS and SCADA vulnerabilities.

• Evaluate the various approaches and best practices used to manage the risks associated with ICS/SCADA vulnerabilities across the critical infrastructure community.

**2. Discussion Topics**

• What is ICS/SCADA? How does ICS/SCADA relate to the critical infrastructure sectors?

• What are the principal threats to ICS/SCADA? How do these threats manifest themselves?

• Does unauthorized access to ICS/SCADA represent a real and present danger?

Why or why not?

• How do the various critical infrastructure sectors address the issues associated with ICS/ SCADA vulnerabilities?

• What are the various approaches to effective ICS/SCADA risk management at the sector level? What are some examples of relevant best practices?

• How do critical infrastructure partners communicate and coordinate with one another to jointly address ICS/ SCADA vulnerabilities?

• What is the DHS CSSP? What are its major elements, products, and services?

• What is the DHS ICSJWG? What are its major subgroups?

• What are the principal elements of the DHS *Roadmap to Secure Industrial Control*

*Systems*?

**3. In-class Exercise:** Learners will consult the Industrial Control Systems Cyber Emergency

Response Team (ICS-CERT) Recommended Practices website

at <http://ics-cert.us-cert.gov/Recommended-Practices>

*Be prepared to discuss an ICS security best practice in detail.*

**4. Required Reading:**

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.](http://energy.sandia.gov/wp/wp-content/gallery/uploads/SustainableSecurity.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.](http://www.gao.gov/new.items/d04354.pdf)

Stouffer, Falco, and Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and*

*Industrialized Control Systems Security*, (2006), Chapters 1-4.

<http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>

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

George Mason University, The Center for Infrastructure Protection and Homeland Security,

*The CIP Report*, 7(8), (February 2009), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_February2009_SCADA.pdf>

Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, (2010), Chapters 1-7, and 12-15.

U.S. Department of Homeland Security, Recommended Practices for ICS Security, <http://ics-cert.us-cert.gov/Recommended-Practices>

**5. Recommended Reading**

Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems Security*, Special Publication 800-82, National Institute of Standards and Technology, (June

2011), <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>

U.S. Department of Homeland Security, U.S. CERT, Control Systems Security

Program, <http://www.us-cert.gov/control_systems/csstandards.html>.

**LESSON 6 TOPIC: ASSESSING AND MANAGING CYBER RISK AT THE SECTOR LEVEL**

**1. Lesson Goals/Objectives:**

• Analyze the cybersecurity landscapes of the various critical infrastructure sectors, including cyber dependencies/interdependencies with other sectors.

• Critique the various sector-level approaches to cybersecurity, including sector best practices.

**2. Discussion Topics:**

• How does the cybersecurity landscape vary across the critical infrastructure sectors? Are some sectors more dependent on cyber systems than others? In what important ways?

• How do cross-sector cyber dependencies/interdependencies affect the security and resilience of the critical infrastructure sectors?

• What are the various sector-level approaches to cyber risk assessment and management? How are they similar? How are they different?

• What are the strengths and weaknesses associated with the various sector-level approaches to cybersecurity?

• Are there cross-cutting cyber best practices that may be effectively applied at the sector level?

**3. In-class Exercise:** Learners will be required to provide an oral critique of the cybersecurity aspects of the various NIPP Sector Specific Plans or sector-level cybersecurity roadmaps, focusing on the following:

• Sector cyber systems and cybersecurity landscape

• Sector approach to cyber risk assessment and management

• Sector approach to ICS security

• Sector approach to cyber dependencies/interdependencies with other sectors

• Strengths, weaknesses, and recommendations.

The instructor will assign topics to 2-person teams at the end of class in Lesson 5. No formal presentations will be required. Critiques will form part of learners’ classroom discussion scores. Information pertaining to the SSPs and additional suggested readings for some sectors are provided below. Depending on the sector assigned, learners may have to undertake additional on-line research to prepare for the classroom discussion.

**4. Suggested Reading:**

NIPP Sector Specific Plans at [www.dhs.gov/sector-specific-plans](http://www.dhs.gov/sector-specific-plans)

U.S. Government Accountability Office, *Sector Specific Plans’ Coverage of Key Cyber Security* *Elements Varies*, (October 31, 2007), [http://www.gao.gov/new.items/d0864t.pdf.](http://www.gao.gov/new.items/d0864t.pdf)

Water Sector Coordinating Council Cyber Security Working Group, *Roadmap to Secure Control* *Systems in the Water Sector*, (March 2008),

<http://www.awwa.org/Portals/0/files/legreg/Security/SecurityRoadmap.pdf>

Rick Dakin, Richard Newman, and Daniel Groves, *“*The Case for Cyber Security in the Water Sector,” *Journal of the American Water Works Association*, (December 2009), <http://www.awwa.org/publications/journal-awwa/abstract/articleid/22455/issueid/33568034.aspx?getfile=/documents/dcdfiles/22455/waternet.0071197.pdf>

U.S. Department of Homeland Security, *Roadmap to Secure Control Systems in the Chemical*

*Sector*, (September, 2009), <http://www.dhs.gov/xlibrary/assets/chemsec_summit_2010_implementation_roadmap_eric_cosman.pdf>

Association of Dam State Safety Officials,

*Dams Sector Roadmap to Secure Control Systems*, (2010), [http://www.damsafety.org/media/Documents/Security/DamsSectorRoadmaptoSecureCon](http://www.damsafety.org/media/Documents/Security/DamsSectorRoadmaptoSecureControlSystems2010.pdf) [trolSystems2010.pdf.](http://www.damsafety.org/media/Documents/Security/DamsSectorRoadmaptoSecureControlSystems2010.pdf)

North American Electric Reliability Corporation, *Critical Infrastructure Strategic Roadmap*, (November, 2010), <http://ccpic.mai.gov.ro/docs/NERC_ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf>

Energy Sector Control Systems Working Group, *Roadmap to Secure Energy Delivery Systems*

(Draft), (January 11, 2011), [http://www.controlsystemsroadmap.net/pdfs/2011\_roadmap\_draft.pdf.](http://www.controlsystemsroadmap.net/pdfs/2011_roadmap_draft.pdf)

U.S. Department of Energy, *Working to Achieve Cybersecurity in the Energy Sector*, (Briefing), (Spring 2011), [http://www1.eere.energy.gov/femp/pdfs/ns/fupwg\_spring11\_wells.pdf.](http://www1.eere.energy.gov/femp/pdfs/ns/fupwg_spring11_wells.pdf)

**LESSON 7 TOPIC: PARTNERING AND SHARING INFORMATION TO MANAGE CYBER RISK**

**1. Lesson Goals/Objectives:**

• Identify the various stakeholders involved in cybersecurity and the responsibilities of each.

• Explain how cybersecurity-related information is collected, warehoused, protected, and exchanged among various levels of government and the private sector.

• Identify and evaluate the ongoing challenges and barriers to cyber information sharing and collaboration that exist among the various levels of government, as well as between government and the private sector.

**2. Discussion Topics:**

• Who is “in charge” of cybersecurity nationally, regionally, locally, and across the critical infrastructure sectors?

• What are the key roles and responsibilities of the following with respect to cybersecurity: Federal, State, local, tribal, and territorial governments; industry; academia; research & development entities; and NGOs?

• How is each of the above players advantaged/disadvantaged regarding these roles and responsibilities?

• What is the role of the Department of Defense (DoD), and, more specifically U.S. Cyber Command or CYBERCOM, in cybersecurity? How do DoD entities with cybersecurity responsibilities interact with DHS?

• What are the principal roles, responsibilities, and functions of the Information Technology ISAC (IT-ISAC) and the Multi-State ISAC (MS-ISAC) regarding cybersecurity? How are they organized and who are their major stakeholders? What are examples of the products and services they provide?

• How do the various government and private entities with cybersecurity responsibilities at different levels interact and collaborate with one another? What processes/systems are used to enable this interaction? What role do the ISACs play in this interaction?

• How are the critical infrastructure sectors organized to accomplish the cybersecurity mission at the sector and sub-sector level?

• How does the distributed structure of cybersecurity authority, responsibility, and accountability play out against the principal threats we face?

• What are the motivations/incentives that drive government-private cybersecurity-related information sharing? What are the criteria used by the private sector to assess the value of collaborative information sharing with the government at various levels?

• What are the principal barriers to sharing cybersecurity-related information proactively and comprehensively between government and industry at all levels of the NIPP partnership?

• How is classified cybersecurity-related information shared between government and industry?

• How do government and industry work together to protect sensitive cyber-related information? Are there areas for improvement?

• How has real-world successes/failures led to improvements in cyber-related information sharing among government and industry partners?

**3. Required Reading:**

Sue Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector*,

(2006), [http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabid=233.](http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabid=233)

*NIPP 2013 Supplemental Tool: Connecting to the NICC and the NCCIC,* http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement\_Connecting%20to%20the%20NICC%20and%20NCCIC\_508.pdf

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.](http://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing* *Strategies and Developing Options for U.S. Policy,* National Academies Press, (2010), 245-272, [http://www.nap.edu/catalog/12997.html.](http://www.nap.edu/catalog/12997.html)

The Comprehensive National Cybersecurity Initiative, (2010), [http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.](http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)

DHS: Office of Cybersecurity and Communications:

[www.dhs.gov/office-cybersecurity-and-communications](http://www.dhs.gov/office-cybersecurity-and-communications)

Information Technology Information Sharing and Analysis Center, <http://www.it-isac.org/>

Multi-State Information Sharing and Analysis Center, [http://msisac.cisecurity.org/.](http://msisac.cisecurity.org/)

InfraGard, <http://www.infragard.net/.>

US-CERT, [http://www.us-cert.gov.](http://www.us-cert.gov/)

ICS-CERT, <https://ics-cert.us-cert.gov/>.

Homeland Security: Protecting, Analyzing & Sharing

Information, <http://www.dhs.gov/sites/default/files/publications/Policy-PSO/private_sector_resource_catalog_December_2012.pdf>

**LESSON 8 TOPIC: SPECIAL TOPICS IN CYBERSECURITY**

**1. Lesson Goals/Objectives:**

• Describe how the cyber threat environment has impacted traditional notions of national sovereignty and international legal norms.

• Assess how cybersecurity impacts civil liberties, privacy, and privacy compliance issues.

• Analyze the challenges associated with the protection of sensitive information in the context of cybersecurity.

• Evaluate the technical, legal, and policy challenges associated with achieving cyber threat attribution.

• Describe the issues associated with a regulatory approach to cybersecurity.

**2. Discussion Topics:**

• How has the emergent cyber threat environment impacted traditional notions of national sovereignty?

• What are the principal legal issues associated with achieving cybersecurity in an interconnected global economy?

• How do cyber attacks across the spectrum of malicious actors and corresponding response options relate to the principles established by the Law of Armed Conflict?

• How does cybersecurity affect traditional notions of civil liberties and privacy, particularly in regard to search, surveillance, and seizure? How do we achieve an appropriate balance between protection and privacy given the advanced cyber threats we face?

• What are the various challenges associated with the protection of sensitive information in the context of cybersecurity partnerships? How is sensitive information protected under existing compliance statutes? Is this regime adequate?

• What are the principle elements of cyber attack attribution? Why does attribution pose such a difficult problem? What solutions are available from a technical, policy, and legal perspective?

• What are the principal issues associated with a regulatory approach to cybersecurity?

What are the costs and benefits of such an approach? How would a regulatory approach impact global commercial concerns?

• How would liability and information disclosure options fit within a regulatory construct?

**3. Required Reading:**

John W. Rittinghouse and William M. Hancock, *Cybersecurity Operations Handbook*, Elsevier Digital Press, (2003), Chapter 1.

Linda Volonino and Stephen R. Robinson, *Principles and Practice of Information Security*, Pearson Prentice Hall, (2004), Chapter 11.

National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing*

*Strategies and Developing Options for U.S. Policy,* National Academies Press, (2010), 3-24,

25-54, 99-150, 151-178, 273-312, [http://www.nap.edu/catalog/12997.html.](http://www.nap.edu/catalog/12997.html)

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>.

Saadewi Tarek and Louis Jordan, Jr. (eds), *Cyber Infrastructure Protection*, U.S. Army War College, (May 2011), Chapter 6.

4th Amendment, [http://www.law.cornell.edu/anncon/html/amdt4toc\_user.html.](http://www.law.cornell.edu/anncon/html/amdt4toc_user.html)

*Katz v. United States*, 389 U.S. 347 (1967), [http://www.law.cornell.edu/supct/html/historics/USSC\_CR\_0389\_0347\_ZS.html.](http://www.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZS.html)

**LESSON 9 TOPIC: THE INTERNATIONAL DIMENSION OF CYBER SECURITY**

**1. Lesson Goals/Objectives:**

• Evaluate the complexities of the international information environment and associated stakeholder relationships.

• Identify and describe the various alternative approaches to cybersecurity in use internationally, including official U.S. government strategy and policy.

• Critique the various structures, forums, and agreements that are used to promote international cybersecurity cooperation and collaboration.

**2. Discussion Topics:**

• How do cyber realities and issues impact international security?

• What does the NIPP have to say regarding the international dimensions of cybersecurity?

• Why do we need to press for secure networks and information access outside our own borders? How do e-supply chain considerations factor into this equation?

• Who are our principal international cybersecurity partners? Are there any outliers?

• How do we achieve cybersecurity in the context of a global economy and the Internet?

• Is there an international standard for cybersecurity? Should there be?

• What are the typical approaches to cybersecurity used outside the United States? What are their strengths and weaknesses? Are these primarily regulation driven or is a voluntary approach used?

• What are the principal agreements that govern cybersecurity internationally? Are they effective? What are their strengths and weaknesses?

• How can international cybersecurity cooperation be enhanced from a technical, legal, and policy perspective?

• Is there an appropriate governance structure(s) through which international cybersecurity and resilience issues can be addressed?

• Is there a national, bi-national, or multi-national cybersecurity program that stands out as a model or best practice?

• How can multi-lateral international cybersecurity cooperation and collaboration be incentivized?

• What are the major elements of the 2011 International Cyber Security Strategy issued by the White House? How will the various aspects of this strategy be implemented and through what mechanism? How will success be measured? Will this be effective? Why or why not?

**3. Required Reading:**

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.](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf) [pdf.](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (eds), *Cyberpower and National*

*Security*, National Defense University Press, (2009), Chapter 14.

European Commission, *Protecting Europe from Large-scale Cyber Attacks and Disruptions: Enhancing Preparedness, Security and Resiliency*, (2009),

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:NOT>

Peter Sommer and Ian Brown, *Reducing Systemic Cyber Security Risk,* Organization for Economic

Cooperation and Development (OECD) Project on Future Global Shock, (January 14,

2011), [http://www.oecd.org/dataoecd/57/44/46889922.pdf.](http://www.oecd.org/dataoecd/57/44/46889922.pdf)

National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing*

*Strategies and Developing Options for U.S. Policy,* National Academies Press, (2010),

179-206. [http://www.nap.edu/catalog/12997.html.](http://www.nap.edu/catalog/12997.html)

**4. Recommended Reading**:

European Network and Information Security Agency, *Member States Need Holistic Cyber*

*Security Strategies*, (February 24, 2010),

[http://www.enisa.europa.eu/media/news-items/v2member-states-need-holistic-cyber-secu](http://www.enisa.europa.eu/media/news-items/v2member-states-need-holistic-cyber-security-strategies) [rity-strategies.](http://www.enisa.europa.eu/media/news-items/v2member-states-need-holistic-cyber-security-strategies)

International Cyber Security Legal and Policy Proceedings, 2010 Conference on Cyber Conflict

Law and Policy Track, (2010), [http://www.ccdcoe.org/245.html.](http://www.ccdcoe.org/245.html)

Enekin Tikk, “Ten Rules for Cyber Security,” *Survival*, 53(3), (June-July 2011), <http://www.tandfonline.com/doi/full/10.1080/00396338.2011.571016#preview>

International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC), The ISO/IEC 27000 Family of Information Security Standards, [http://www.iso.org/iso/pressrelease.htm?refid=Ref1223.](http://www.iso.org/iso/pressrelease.htm?refid=Ref1223)

Australian Government Cyber Security Strategy (2009),

<http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf>

Cyber Security Strategies for Germany, Holland, and France, [http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-present](http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-presented) [ed.](http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-presented)

United Kingdom Cyber Security Strategy, [http://www.cabinetoffice.gov.uk/content/cyber-security.](http://www.cabinetoffice.gov.uk/content/cyber-security)

Reporting and Analysis Centre for Information Assurance MELANI, [http://www.melani.admin.ch/index.html?lang=en.](http://www.melani.admin.ch/index.html?lang=en)

International Code of Conduct for Information

Security, [http://www.rusemb.org.uk/policycontact/49.](http://www.rusemb.org.uk/policycontact/49)

**5. Additional Activity (Optional)**:

Search for cybersecurity strategies for countries not listed above.

**LESSON 10 TOPIC: CYBER INCIDENT RESPONSE**

**1. Lesson Goals/Objectives:**

• Identify and describe the fundamentals of cyber incident response and its role within an effective cybersecurity program.

• Assess the effectiveness of the cyber incident response team (CIRT), cyber emergency response team (CERT), and related coordinating structures, reporting processes, and products as they relate to cyber incident response.

• Describe the National Cyber Alert System and how it functions.

• Explain the process of developing plans, protocols, and procedures for cyber incident response across various incident types.

**2. Discussion Topics:**

• What is the fundamental purpose of a cyber incident response program? Why does an organization need a strong incident response program?

• What is a CIRT/CERT? How does it function?

• What types of stakeholders are typically included in a CIRT/CERT structure? What are their typical roles and responsibilities?

• What is the US-CERT? How is it organized and resourced?

• What are the coordinating structures and processes that the US-CERT uses to manage the response to cyber incidents? How are cyber threats/incidents and vulnerabilities reported and acted upon within the US-CERT framework?

• What are some examples of typical products produced by the US-CERT?

• Who are the principal partners of the US-CERT?

• What is the National Cyber Alert System and how does it work?

• How does the CIRT/CERT concept apply to the management of ICS/SCADA-related incidents?

• What is the DHS ICS-CERT? What are its major functions, products, and services?

• How do computer forensics relate to cyber incident response?

• What are some of the legal issues associated with cyber incident response?

**3. In-class Exercise:** Learners will be required to provide a brief synopsis of a specific cyber threat or vulnerability as posted on the US-CERT or ICS-CERT website and discuss relevant mitigation measures and stakeholder awareness activities.

**4. Required Reading:**

Linda Volonino and Stephen R. Robinson, *Principles and Practice of Information Security*, Pearson Prentice Hall, (2004), Chapter 7.

John W. Rittinghouse and William M. Hancock, *Cybersecurity Operations Handbook*, Elsevier Digital Press, (2003), Chapters 10, 11 and 13.

Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, (2010), Chapters 9 and 11.

US-CERT, [http://www.us-cert.gov.](http://www.us-cert.gov/)

ICS-CERT, <http://www.us-cert.gov/nccic/>

U.S. Department of Homeland Security, U.S. CERT, National Cyber Awareness

System, <http://www.us-cert.gov/ncas>

Multi-State Information Sharing and Analysis Center, Cyber Incident Response Guide, [http://msisac.cisecurity.org/resources/guides/documents/Incident-Response-Guide.pdf.](http://msisac.cisecurity.org/resources/guides/documents/Incident-Response-Guide.pdf)

American Bar Association Cyber Crime Committee, [http://www2.americanbar.org/sections/criminaljustice/CR107500/Pages/default.aspx](http://www2.americanbar.org/sections/criminaljustice/CR107500/Pages/default.aspx?com=CR107500)

[?com=CR107500.](http://www2.americanbar.org/sections/criminaljustice/CR107500/Pages/default.aspx?com=CR107500)

**LESSON 11 TOPIC: MANAGING NATIONAL CYBER INCIDENTS**

**\*\*SPECIAL ACTIVITY**: **CYBER INCIDENT MANAGEMENT EXERCISE PREPARATION**

Today’s class involves a “walk-through” of the national cyber incident response processes and coordinating structures that will form the basis of next lesson’s interactive, discussion-based table top exercise (TTX). This lesson will provide an understanding of the National Response Framework (NRF) and the National Cyber Incident Response Plan (NCIRP) as they apply to critical infrastructure security and resilience. This lesson will also explore the relationship between the NIPP, the NCIRP, and the NRF in detail, including an examination of how the government and private sectors share information, maintain situational awareness, and provide assistance to one another during cyber incidents affecting the critical infrastructure sectors. This scenario will consist of three modules (Pre-incident, Incident Response, and Recovery), portraying a series of malicious cyber attacks against interconnected critical infrastructure systems in multiple sectors and regions of the United States. The TTX will focus on the roles, responsibilities, and interaction between Federal, State, local, tribal, and territorial governments; the private sector; and the general public in the context of an emergent cyber threat as well as an incident in progress. Participant discussion will focus on communication and information sharing, coordination, integration of capabilities, and problem identification and resolution.

**1. Lesson Goals/Objectives:**

• Summarize the purpose and scope of the NRF Cyber Incident Annex and the

NCIRP.

• Assess government-private sector information sharing and intelligence in the context of cyber incident management.

• Evaluate the processes and mechanisms used to build situational awareness and facilitate government-private cyber-related prevention, protection, mitigation, response, and recovery activities.

**2. Discussion Topics:**

• What are the major components of the cyber incident response life cycle as discussed in the

NCIRP?

• What is the national concept of operations for cyber incident response as discussed in the NCIRP? How is a common operating picture for cyber incident response maintained according to this CONOPS?

• What are the roles and responsibilities of the various government and private sector partners vis-à-vis national cyber incident management?

• What are the primary coordinating and cooperating agencies for cyber response as discussed in the NRF Cyber Incident Annex? How do they interact?

• What are the key government and private sector incident management nodes as discussed in the NRF Cyber Incident Annex and the NCIRP? What are the structures and process used to govern their interaction?

• What is the National Cyber Security and Communications Coordination Center? What role does it play across the cyber incident response life cycle? How is it structured and how does it function? How does it tie into US-CERT and ICS-CERT?

• How is information and intelligence shared between the various public and private sector nodes of the NIPP Partnership Framework in an emergent cyber threat scenario? Does the process work?

• What actions do the sectors take in response to a national level NTAS elevation? How does this process work? What are the near and long-term ramifications across the sectors?

• How is situational awareness maintained among the various NIPP partners during cyber incident response?

• How are private sector issues assessed and addressed during cyber incident response operations?

**3. Required Reading (for Lessons 11-12):**

U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, (2013), pp. 35-40, Appendix A, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

U.S. Department of Homeland Security, *Overview of the National Planning Frameworks*, (May 2013). <http://www.fema.gov/media-library-data/20130726-1914-25045->2057/final\_overview\_of\_national\_planning\_frameworks\_20130501.pdf

U.S. Department of Homeland Security, *Cyber Incident Annex to the National Response*

*Framework*, (2004), <http://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf>

U.S. Department of Homeland Security, *Critical Infrastructure/Key Resource Support Annex to the National Response Framework*,

(2008), [http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf.](http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf)

FEMA, IS 821.A, *Critical Infrastructure Key Resource Support Annex*, (2013), <http://training.fema.gov/EMIWeb/IS/IS821.asp.>

U.S. Department of Homeland Security,

*National Cyber Incident Response Plan (Interim Version)*, (September

2010), [http://www.federalnewsradio.com/pdfs/NCIRP\_Interim\_Version\_September\_2010.pdf.](http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf)

National Infrastructure Advisory Council,

*Framework for Dealing with Disasters and Related Interdependencies*, (July

2009), [http://www.dhs.gov/xlibrary/assets/niac/niac\_framework\_dealing\_with\_disasters.pdf.](http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealing_with_disasters.pdf)

National Terrorism Advisory System, [http://www.dhs.gov/files/programs/ntas.shtm.](http://www.dhs.gov/files/programs/ntas.shtm)

**4. Additional Recommended Reading:**

*National Incident Management System*,

(2008), [http://www.fema.gov/pdf/emergency/nims/NIMS\_core.pdf.](http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf)

*National Response Framework*, (2013), <http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf>

FEMA, IS 800.B, *National Response Framework: An Introduction*, (2013), [http://www.training.fema.gov/EMIWeb/IS/IS800b.asp.](http://www.training.fema.gov/EMIWeb/IS/IS800b.asp)

**LESSON 12 TOPIC: NATIONAL CYBER INCIDENT MANAGEMENT EXERCISE**

**\*\*SPECIAL ACTIVITY:**

**CYBER INCIDENT MANAGEMENT POINT PAPERS DUE VIA EMAIL PRIOR TO CLASS**

Today’s class involves an interactive, discussion-based table top exercise (TTX) driven by a malicious actor. This scenario will consist of three modules (Pre-incident, Incident Response, and Recovery), portraying a series of attacks against cyber systems forming key components of critical infrastructure systems across multiple sectors and regions of the United States. The TTX will focus on the roles, responsibilities, and interaction between Federal, State, local, tribal, and territorial governments; the private sector; and the general public in the context of an emergent cyber threat as well as a cyber incident in progress. Participant discussion will focus on communication and information sharing; coordination, integration of capabilities; and problem identification and resolution. A complete outline of the exercise scenario and module discussions is provided in **Attachment 1**.

**1. Lesson Goals/Objectives:**

• Apply course themes in the context of a comprehensive cyber incident management TTX.

**2. Discussion Topics:**

• See Attachment 1.

**3. Required Reading:**

* See Lesson 11

**LESSON 13 TOPIC: MANAGING FUTURE CYBER RISK TO CRITICAL INFRASTRUCTURE**

**1. Lesson Goals/Objectives:**

• Describe the potential future cyber operating and security risk landscapes and related challenges.

• Explain how the complex technical, economic, and social elements associated with the

Internet may change over time.

• Analyze the various strategic choices that may impact our approach to cybersecurity in the medium-long term future (10-20 years from now).

**2. Discussion Topics:**

• What will the critical infrastructure and cybersecurity operating environments look like

10-20 years from now? What will the global information and information technology environments look like in 10-20 years? What are the major technical, economic, and social trends that will most likely drive this evolution?

• What will be the principal threats and challenges to critical infrastructure and cyber systems in the future?

• How might we best integrate cybersecurity considerations into future critical infrastructure security and resilience planning?

• What would constitute the core elements of a future cybersecurity strategic framework?

• How are cybersecurity-related requirements determined and resourced within government? Industry? Across sectors? Are these processes sufficient to get us ready for the future?

• How can we achieve truly integrated government-private cybersecurity planning and risk management in the future? How can cybersecurity goals and objectives be harmonized and administered within and across sectors, jurisdictions, and geographic regions?

• How might we be better able to measure cybersecurity performance in the future?

• How do we begin to address cybersecurity concerns that transcend the next budget cycle?

• What actions should we be taking now to buy down future cyber-related risk and position the next generation for success in this area? Will today’s priorities set us up for future success?

• What are the core elements of an effective cyber critical infrastructure awareness, education, and training program? And at what levels should these be taught?

• What are some of the major challenges associated with developing cyber course curricula?

How do the legal, technical, and policy issues discussed in Lesson 8 come into play here?

• How effective are major exercises like the Cyber Storm series in promoting cyber awareness and issue resolution? What have been some of the major lessons learned from

these types of exercises?

• What are some of the important keys to effective cybersecurity policy, strategy, and program management today, tomorrow, and in the future?

• Can the future world of cybersecurity be simulated and “war-gamed” today?

• Is cybersecurity a legitimate future concern? Why or why not?

• How will future cybersecurity threats manifest themselves? Food? Water? Environment?

Could there be multiple threats? If so, how can we ensure that we consider all future threats as opposed to focusing on the most current threat?

**3. Required Reading:**

John W. Rittinghouse and William M. Hancock, *Cybersecurity Operations Handbook*, Elsevier Digital Press, (2003), Chapter 18.

Toffler Associates, *Guarding Our Future: Protecting our Nation’s Infrastructure*, (2008), [http://www.toffler.com/docs/Guarding-Our-Future.pdf.](http://www.toffler.com/docs/Guarding-Our-Future.pdf)

Toffler Associates, *Five Critical Threats to the Infrastructure of the Future*, (2008). [http://www.toffler.com/docs/Five-Critical-Infrastructure-Threats.pdf.](http://www.toffler.com/docs/Five-Critical-Infrastructure-Threats.pdf)

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (eds), *Cyberpower and National*

*Security*, National Defense University Press, (2009), Chapters 3 and 8.

Tarek Saadewi and Louis Jordan, Jr., (eds), *Cyber Infrastructure Protection,* U.S. Army War

College, (May, 2011), Chapter 12.

Rand Corporation, *Cyber-terrorism: The Threat of the Future?* Rand Corporation Summary

Report, <http://www.rand.org/pubs/reprints/RP1051.html>

Center for Strategic and International Studies, *Cyber Security Two Years Later,* Report of the CSIS Commission on Cyber Security for the 44th Presidency, Washington, D.C., (January 2011).

U.S. Department of Homeland Security, Cyber Storm: Securing Cyber

Space, [http://www.dhs.gov/files/training/gc\_1204738275985.shtm.](http://www.dhs.gov/files/training/gc_1204738275985.shtm)

**4. Additional Activity (Optional): Think-Pair-Share**

Learners will pair up with their “shoulder” partner (closest neighbor) to discuss the future concerns

of cybersecurity with regards to critical infrastructure security, including concerns/ideas that appear to be outside the “realm of the possible” at this point in time. Discussion of scenarios described in books and films are encouraged. Why are some scenarios more likely than others? Report to the class.

**LESSON 14 TOPIC: RESEARCH PAPER PRESENTATIONS**

**1. Lesson Goals/Objectives:**

• Provide a concise analysis of a cybersecurity issue and provide recommendations for improvement (Problem-Discussion-Recommended Solution format) **or**

• Provide a concise synopsis of a recommended cyber risk assessment and management strategy for a specific infrastructure sector, sub-sector, or system.

• Provide constructive feedback to peers on their analysis.

• Summarize and discuss lessons learned and observations from presentations.

• Provide a forum for learner feedback on overall course content, method of instruction, and flow.

**2. Discussion Topics:**

• Presentations.

**3. Required Reading:**

• As required for research paper and presentation.

**LESSON 15 TOPIC: RESEARCH PAPER PRESENTATIONS AND COURSE WRAP-UP**

**\*\*SPECIAL ACTIVITY: FINAL RESEARCH PAPERS ARE DUE VIA E-MAIL PRIOR TO CLASS**

**1. Lesson Goals/Objectives:**

• Provide a concise analysis of a cybersecurity issue and provide recommendations for improvement (Problem-Discussion-Recommended Solution format) **or**

• Provide a concise synopsis of a recommended cyber risk assessment and management strategy for a specific infrastructure sector, sub-sector, or system.

• Provide constructive feedback to peers on their analysis.

• Summarize and discuss lessons learned and observations from presentations.

• Provide a forum for learner feedback on overall course content, method of instruction, and flow.

**2. Discussion Topics:**

• Presentations.

• Course Evaluation: Course content, flow, instructional methodology, etc.

**3. Required Reading:**

• As required for research paper and presentation.

**ATTACHMENT 1**

**NATIONAL CYBER INCIDENT MANAGEMENT EXERCISE**

**MODULE 1: EMERGENT THREAT**

**1. Scenario Build**

• **General Threat Background**: A politically motivated computer hacker organization calling itself the Global Anti-Western Coalition (GAWC) has been active for several years. The GAWC is committed to undermining the governments and industries of the United States, Western Europe, and Japan as a result of alleged “government-industry capitalist collusion and decadent mismanagement of the world’s economy to the detriment of hundreds of millions of impoverished people around the globe.” GAWC is thought to be highly decentralized with dozens of individual affiliates and hundreds of sympathizers operating under a loose umbrella network worldwide, with particularly strong support within the Middle East, Southwest Asia, and Southeast Asia. The group has demonstrated an increasingly sophisticated “offensive” cyber capability over the years and has claimed responsibility for numerous cyber penetrations, website defacements, and denial of service attacks against prominent banking and finance institutions, the oil and gas industry, the petrochemical industry, and various Federal agencies, including the Departments of State, Commerce, and Energy and the Internal Revenue Service. An Internet video recently released by GAWC reaffirms the group’s intent to “strike at the heart of the corrupt and decadent Western economic system and the industries that support Western economic power and socio-cultural decay.” In the build-up to the upcoming G-8 Summit in

mid-May of this year, GAWC is calling for “unified international action” to disrupt the event and prevent the recovery of the “existing highly exploitative international economy.” Based on previously successful “calls to action,” it is likely that many GAWC activists and supporters may attempt to disrupt the computer networks and information systems of western governments and industries in the coming months.

• **March 1, 20XX**: A prominent European “hacktivist” reveals the existence of a vulnerability common to the industrial control systems typically employed in the electricity, chemical, oil and gas, water, and manufacturing sectors, both domestically in the United States and internationally. This vulnerability has been named “Achilles” by the international hacker community. The Achilles vulnerability and the potential means to exploit it were principal topics of discussion at an international “hacktivist” convention held this month in Amsterdam. The international media and Internet coverage of this vulnerability is widespread. GAWC-affiliated websites and chat rooms all contain numerous references to the Achilles vulnerability and its potential exploitation. DHS issues a warning regarding this vulnerability and its potential exploitation through the

US-CERT.

• **March 15, 20XX:** In response to the disclosure of the Achilles vulnerability, US-CERT

and its industry partners in the potentially affected sectors issue a list of potential defensive countermeasures/effective practices, including technical remediation products/solutions, vendors, and recommended upgrades.

• **April 15, 20XX**:An FBI cyber crime task force operating out of the Washington Field

Office receives a tip from a credible source regarding potential cyber disruption of the G-8

Summit and simultaneous cyber attack on energy, water, and manufacturing sector industrial control systems aimed at exploiting the Achilles vulnerability.

• **April 18, 20XX**: DHS and the FBI issue a joint warning discussing the need to be prepared for potential large-scale cyber disruptions in protest of the upcoming G-8

Summit. A separate, more specific warning is issued to the electric, chemical, oil and gas, water, and manufacturing sectors focusing on the potential for an attack on industrial control systems within those sectors timed to coincide with the G-8 summit.

• **May 1, 20XX**: There is tremendous angst among the cyber and industrial control systems user communities as the G-8 Summit draws closer. Patches and other remediation measures have been employed throughout various critical infrastructure sectors, but the exact nature of the threat and extent of the Achilles vulnerability remain largely unknown. DHS and the FBI have reason to believe through numerous email intercepts that some of the security upgrades recommended to mitigate the Achilles vulnerability may have actually contained malware disguised as legitimate software, with the GAWC as the likely perpetrator of this tactic. Apprehension within the cyber community spikes as confidence in remediation measures plummets across the affected sectors. The exact nature of the malware and specific products affected remains unknown.

• **May 5, 20XX:** GAWC websites and chat rooms reaffirm the previous “call to action” regarding disruption of the G-8 summit and a “call to arms” regarding Western governments and industry. The GAWC “virtual” leadership proclaims that “[s]oon the world will realize the extent of the ‘hollow shell’ of Western capitalism.”

• **May 10, 20XX:** DHS, the FBI, and numerous large-size energy companies receive faxes and emails from anonymous sources warning of pending attacks on information systems and industrial control systems, Internet disruptions, and virtual “sit-ins” of major government and corporate websites.

**2. Discussion Questions**

• How would cyber attacks perpetrated by GAWC be distinguished from everyday cyber

“white noise” from a U.S. government or private sector perspective?

• How would the various nodes and coordinating structures detailed in the NRF Cyber

Incident Annex and the NCIRP come together in response to the GAWC threat?

• What actions would the U.S. government/industry take in response to the GAWC Internet-based proclamations in early March? In response to the GAWC proclamations and variety of additional threat information received in the two weeks prior to the kickoff of the G-8 Summit?

• What is the role of the National Cyber Security and Communications Coordination Center

(NCSCCC) in the context of this scenario?

• How would the response to this emergent threat differ from the “steady-state” cyber response baseline at the national level?

• How would your organization be alerted to a cyber threat?

• How would DHS and the FBI interact with one another in response to the CAWC threat?

• What type of information regarding the threat posed by GAWC would be shared and how would it be shared? Between government agencies? Between government and industry? Between the U.S. and other governments internationally?

• What actions would the U.S. government/industry take in response to the discovery of the Achilles vulnerability? What is the specific role of the ICS-CERT and the various sector ISACs in dealing with this vulnerability?

• How would key information related to GAWC tactics, techniques, and procedures be disseminated throughout the cyber user community?

• How would the National Cyber Alert System (NCAS) factor into the emergent threat situation represented by GAWC? Would this scenario cause the NTAS to be elevated? Is there a specific relationship between the NCAS and NTAS?

• What types of protective measure enhancements would be implemented by the NIPP Partnership across the critical infrastructure sectors based on the GAWC threat and the Achilles vulnerability?

• What prevention/protection activities would your jurisdiction/agency/sector engage in at this time?

• How would the public message regarding the GAWC threat and the Achilles vulnerability be developed, coordinated, and disseminated? Who has the lead regarding public messaging and national cyber incidents?

**MODULE 2: OPERATIONAL RESPONSE**

**1. Scenario Build**

• **May 15, 20XX (Opening day of the G-8 Summit)**:

o The virtual sit-in previously announced by GAWC begins mid-morning. The websites and Internet communications of numerous major oil and gas, chemical, and manufacturing corporations are disrupted; some are experiencing major denial of service attacks. The official websites and Internet communications of the U.S. Departments of Energy and Commerce are similarly affected. System administrators in the affected industries and government agencies are attempting to resolve the issues. Additionally, all coordination and response nodes detailed in the NCIRP are fully staffed and mobilized; Federal interagency coordination and coordination between US-CERT and affected industry cyber attack response organizations is in full swing.

o As the day progresses, the ongoing cyber attack and service disruptions begin to receive focused media attention, supported by a deep pool of on-air “cybersecurity” experts and commentators. The intensifying media coverage begins to alarm household and community business Internet users regarding the security of their personal computer systems and Internet communications. Worried callers begin to overload government cyber “hotlines.”

• **May 16, 20XX (Day 2 of the G-8 Summit)**:

o Continued disruption of major corporate websites is expected to cost the various affected industries tens of millions of dollars in lost revenue. Numerous websites have been deliberately taken offline to allow the application of patches and other remediation measures. The GAWC has posted an announcement on its website claiming responsibility for the disruption of government and corporate websites and Internet communications.

o The North American Electric Reliability Corporation (NERC) reports that several remote, unmanned power generating stations on the East Coast are experiencing sporadic real time generation data feed failure and faulty emergency readings on key transmission system elements for no apparent reason. Additionally, numerous substations are reporting erroneous voltage data readings.

o Several major East Coast petrochemical production facilities and natural gas pipeline operators have reported sporadic disruption of key automated industrial control systems. Although there appears to be no immediate threat to public health and safety at this time, key production and distribution processes are unstable.

o The U.S. government is considering elevating the NCAS with a focus on the energy, chemical, and critical manufacturing sectors.

o Late in the day, breakers on several transmission lines providing power to the greater Philadelphia area have been tripped by malfunctioning ICS components, causing a large power outage affecting major portions of the city. Industry technicians are rerouting electricity to unaffected lines, and the area power provider has begun load shedding operations, causing rolling blackouts in an area affecting several hundred thousand customers. These outages have affected the normal operation of the Philadelphia mass transit system as well as hundreds of traffic lights in congested areas of the city, causing huge traffic disruption/gridlock and mass movements of stranded commuters on foot across the impacted area. The Philadelphia Airport has also suspended operations due to the blackouts, and uncertainty regarding the security of the cyber system supporting regional air traffic control operations. Local and national media area provide continuous coverage of this evolving scenario, attempting to “connect the dots” between this event and the events of earlier in the day. Philadelphia area residents are bombarding the utility and local government emergency management offices with requests for information and assistance and assurances of their safety.

**2. Discussion Questions**

• What are your major personal and organizational concerns and priorities at this point?

• What prevention/protection activities would your jurisdiction/agency/sector engage in at this time?

• How would the various nodes and coordinating structures detailed in the NRF Cyber

Incident Annex and the NCIRP come together in response to the day’s events?

• What would be the nature of any cyber alerts/warnings provided by the Federal government to the private sector and/or State and local government officials at this time? How would this process work?

• How would situational awareness among the various NIPP partners be maintained in this scenario?

• What type of information regarding the response to the day’s sequence of events would be shared and how would it be shared? Between government agencies? Between government and industry? Between the U.S. and other governments internationally?

• What actions would the U.S. government/industry take in response to the “virtual sit-in?

The ICS-focused attacks/disruptions? In response to the GAWC proclamations of responsibility?

• What are the roles of the US-CERT, ICS-CERT, and NSCCCC regarding the day’s events?

• What specific preventive/protective measures would government authorities and targeted elements of the private sector put in place this point? How would they be communicated to one another?

• How would the discussion related to the NCAS elevation be framed? How does this process work?

• In the absence of government guidance or action, would the private sector initiate any changes in protective measures and emergency response posture on its own within the infrastructure sectors of concern in this scenario?

• If so, would these changes be individually considered or would industry within a sector come together collectively and collaborate?

• Beyond cyber response activities, what types of activities would the various key nodes of the NIPP incident management framework engage in at this point?

• How would the public message regarding the response to the various malicious cyber activities occurring throughout the day be developed, coordinated, and disseminated? Who has the lead for public messaging during the response?

**MODULE 3: RECOVERY**

**1. Scenario Build**

• **May 17 (Day 3 of the G-8 Summit):**

o The virtual sit-in appears to have run its course. Most affected government and corporate websites and Internet communications have returned to normal, albeit at a much slower rate of data flow than is the norm. A few corporations are still having difficulties assuming normal information operations. Corporate losses are running unofficially at several hundred million dollars in lost revenues.

o Household Internet users and companies unaffected by the events of the past two days remain apprehensive regarding their vulnerability to potential follow-on attacks.

o The FBI announces the arrest of three men allegedly associated with the cyber attacks/disruptions of the past two days and that their investigation will continue. All three are known “hacktivists” with close ties to the GAWC.

o The identity of the subject malware has been traced to an unwitting vendor; countermeasures are in development and will be disseminated appropriately to the user community.

o ICS experts within the electricity sector have isolated most of the technical issues associated with the ICS disruptions to that sector. Power is slowly being restored to many impacted areas, although more than 150,000 customers remain without power at mid-day. Priority for restoration is being given to life line infrastructures and services.

o ICS experts within the oil and gas, petrochemical, and critical manufacturing sectors are having a more difficult time isolating their ICS issues and applying appropriate work-arounds. Public safety concerns remain high regarding ICS processes associated with toxic materials production and containment.

o The GAWC leadership claims credit for the previous day’s massive power outages and ICS disruptions across numerous critical industries. They announce the existence of additional malware and state that renewed attacks on an even greater scale will take place over the next several weeks. A positive connection between GAWC and yesterday’s events has not been established by the FBI or other cyber authority.

o The national and international impacts of the cyber attacks in the United States have been high, cascading across the sectors domestically and internationally. The stock market has fallen dramatically, with downward trends globally.

o The NCAS remains in “Elevated” status for the affected sectors.

o Public messaging across levels of government and between government and the private sector has confusing over the course of the past two days. Generally speaking, public confidence remains low and apprehension regarding the potential for follow-on cyber disruptions remains high.

• **One week from the attacks in the United States**

o No further attacks have taken place, although GAWC Internet rhetoric is at an all-time high with pronouncements of additional cyber attacks and disruptions on a daily basis. The NCAS is lowered and most sectors return to normal operations.

o Remediation of the Achilles vulnerability will require a focused public-private,

cross-sector effort involving both hardware and software solutions. CERT-ICS issues

recommended Achilles remediation measures to all NIPP partners.

**2. Discussion Questions**

• What are your principal concerns/priorities in this phase of cyber incident management?

• What types of enhanced prevention and protection activities would you continue at this point? Where do you go for help if required?

• What impacts have the changes in the NCAS had on your organization/jurisdiction/constituency?

• What is the “new normal” regarding cybersecurity for your agency, jurisdiction, corporation, or sector at this point?

• What are the lessons that you have learned from this experience in the role that you played, and how will they be applied to your exercise organization?

• How will these lessons learned be used to heighten cybersecurity awareness within your organization/jurisdiction/sector?

• How difficult will it be to implement the Achilles countermeasures within your organization/jurisdiction/sector? What are the principal obstacles to implementation?

• What are the long-term economic and psychological implications of the cyber attacks perpetrated in this scenario from your perspective?

• What does this scenario tell us about key dependencies/interdependencies between the critical sectors from a cyber perspective?

• How do we regain public confidence in the aftermath of a major regional or national level cyber attack/disruption? How is this process managed?

• What are the major lessons that you have learned individually from this exercise?