Carnegie Mellon
Heinz College

<table>
<tr><td>Course Information*</td><td>Course number: 95-761
Meets: Thursdays (5:30p-8:20p)
Location: HBH 236

Professor: Sam Merrell
Office location: CIC Building
Office hours: by appointment
Email: smerrell@cert.org

Please include the course number in your email subject line</td></tr>
<tr><td>Prerequisites</td><td>While no formal prerequisites are in place, having a solid understanding of cybersecurity management concepts is beneficial</td></tr>
<tr><td>Description*</td><td>The US National Infrastructure Protection Plan identifies Critical Infrastructure as “assets, systems, and networks whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.” In the US, critical infrastructure is classified into 16 sectors, and includes thousands of organizations across many industries. Examples of Critical Infrastructure organizations include banks, electric utilities, nuclear power plants, water treatment utilities, and custodians of Internet technologies. Because so much of the nation’s critical infrastructure is privately owned, ensuring its safety and security requires an ongoing and productive partnership between the government and the private sector.
By the end of this mini, you should be able to:
Explain the current state of Critical Infrastructure Protection efforts in the US, with a focus on cybersecurity challenges and successes
Recognize common obstacles to achieving success in CIP efforts, and be prepared to work around those obstacles
Construct components of an enterprise cyber security strategy that is aligned (as much as practicable) with national cyber security policies
The goal of the class is to inform future cybersecurity managers who will work in firms across the 16 Critical Infrastructure Sectors in the U.S. about how they might one day have an important role in national security. By the end of this course, you should be familiar with critical infrastructure protection efforts in the U.S., and how the various sectors have wrestled with cybersecurity. We will examine successes and failures in current efforts, applying concepts of enterprise risk management to identify opportunities to improve these efforts.</td></tr>
<tr><td>Course Materials (if applicable)</td><td>
<table>
<tr><th>Abbreviation</th><th>Full Name</th><th>URL</th></tr>
<tr><td>APT1</td><td>APT1: Exposing One of China’s Cyber Espionage Units</td><td>http://intelreport.mandiant.com/</td></tr>
<tr><td>BestPractices</td><td>Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability</td><td>www.cert.org/archive/pdf/11tr015.pdf</td></tr>
<tr><td>CISPA</td><td>Cyber Intelligence Sharing and Protection Act (CISPA)</td><td>http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR624.pdf</td></tr>
<tr><td>CIOReportGuide</td><td>“CIO CYBERTHREAT RESPONSE & REPORTING GUIDELINES”</td><td>http://www.isaccouncil.org/images/CIO-Cyberthreat-rptg-guide.pdf</td></tr>
<tr><td>CSIS2</td><td>“Cybersecurity Two Years Later”</td><td>http://csis.org/publication/cybersecurity-two-years-later</td></tr>
<tr><td>CSTF</td><td>Cyber Security Task Force: Public-Private Information Sharing</td><td>http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf</td></tr>
<tr><td>EO</td><td>Executive Order, “Improving Critical Infrastructure Cybersecurity”</td><td>http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity</td></tr>
<tr><td>ES-C2M2</td><td>Electricity Subsector Cybersecurity Capability</td><td>http://energy.gov/oe/services/cybersecurity/electricity-subsector-</td></tr>
</table>
</td></tr>
</table>

		Maturity Model	cybersecurity-capability-maturity-model
	GenericFramework	"A Generic National Framework For Critical Information Infrastructure Protection (CIIP)"	http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
	HSPD-7	Homeland Security Presidential Directive -7	http://www.dhs.gov/homeland-security-presidential-directive-7
	International CIIP	"International CIIP Handbook 2008/2009"	http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=91952&lng=en
	ISC	International Strategy for Cyberspace	http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
	NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection Standards	http://www.nerc.com/page.php?cid=2|20
	NIPP	National Infrastructure Protection Plan	http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
	NSISS	National Strategy for Information Sharing and Safeguarding	http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf
	NSSC	National Strategy to Secure Cyberspace	http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
	PDD-21	Critical Infrastructure Security and Resilience	http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
	PDD-63	Presidential Decision Directive – 63	http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
	SSPs	Sector Specific Plans (select one)	http://www.dhs.gov/critical-infrastructure-sectors
	SP-800-55	Special Publication 800-55 "Performance Measurement for Information Security"	http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Evaluation* Method

Your grade will be based on two 4-5 page written assignments and class participation. Each of these will be worth 1/3 of your grade.

ATTENDANCE AND PARTICIPATION

This course consists of lectures, discussions, individual writing exercises, and group projects. Attendance is required. Each week, class attendance is recorded, and contributes ½ of the value of your in-class participation grade.

Moreover, class participation is required – many of the learning objectives depend upon student engagement and the conveyance of thoughts and ideas commensurate with small group dynamics. Engagement is defined as active contribution to classroom discussions and a willingness to accept and offer peer critiques. Class participation will be judged by attendance and your contribution to discussions both in-class and within the Blackboard Discussion Board. I will look for evidence that you have read the assignments, and that you are trying to understand them. I do not expect you to have mastered the material in the readings before the class in which it is discussed, but I do expect you to demonstrate that you are trying to understand it. Further, your participation will make class more enjoyable and a better learning experience for all. While I expect to spend some of each class lecturing, you will learn more and enjoy class more if there is a good level of interaction. Questions and discussion are welcome at any time during the class. Participation in-class is recorded weekly, and contributes the second half of your in-class participation grade. Since class participation is a significant portion of your grade, please let me know if you will miss a class and why. Unexplained absences will count against your grade.

Participation is also expected within the Blackboard Discussion Board for this course. You must contribute a minimum of **two** original posts to the discussion board **per week**. Original posts must consist of your own original words and must be relevant to the topic under discussion. Simply posting links to other articles or documents is insufficient to gain credit for online participation. You must make a salient point. Linked materials can support a point you are making, but the linked content need to be introduced, summarized, and its value explained in your own words in order to gain credit for participation. Avoid pasting entire articles or webpages into your submission; nobody wants to read that, and original formatting is often lost. Please note that discussion board submissions are

	subject to the rules on plagiarism (see "Academic Conduct" below). EVALUATION OF WRITTEN ASSIGNMENTS In grading your written assignments, I will look for how well you have addressed the topic for the paper, and how well you have incorporated the material presented to date, as applicable. I will also look to see how well it is written, as the quality of the paper's content will be clearer if it is well written. I will judge how well it is written by the paper's organization and the proper use of the English language. Editing and grammar count! If you do not proofread your submission, it is likely your grade will suffer. It is your responsibility to answer the questions posed for the assignment, and clearly articulate your ideas and knowledge, and support your positions with evidence and references.. Two thirds of your grade will be based on content, and one third on exposition. We will discuss this during the first class. Your papers must be four to five full pages in length, using times new roman font, 1.5 line spacing and normal margins. Title pages, large graphics, and bibliographies/works cited do not count towards your page limit. Instructions for each assignment will be first reviewed in class and subsequently posted to Blackboard, including the associated grading rubric. Grades are non-negotiable. Grading standards include: • "A" signifies that the content submitted can be distributed in a professional environment without revisions • "A-" denotes that minor revisions are needed prior to distribution • "B+" means that significant revisions are needed, but essentially the documents follow guidelines provided by the instructor; • "B" indicates that extensive revisions are needed and the student did not follow guidelines provided in the textbook or by the instructor; • "B-" or lower conveys that the assignment submitted would not be considered professional and therefore should not be distributed. *Papers that have not been edited, and contain egregious grammatical errors can be awarded B- or lower, regardless of content*. SUBMISSION OF ASSIGNMENTS • Unless otherwise instructed, assignments are to be provided electronically in Blackboard by midnight of their due dates. • If you turn in a written assignment late without a good reason for doing so – which you should discuss with me before the due date for the paper – you will be docked 1/3 of a letter grade for each day it is late. For example, a paper that is one day late and which would have received an A grade will get an A-; if two days late, the same paper would get a B+ grade. CLASSROOM POLICIES You may bring your laptop to class to take notes, but you may not surf the internet or do emails during class. Doing so will result in a lower class participation grade.
Learning/Course Objectives*	1. An Introduction to CIP in the US a. Learning Objectives: At the end of this class, you should be able to: i. Understand the history of Critical Infrastructure in the US ii. Identify important cybersecurity incidents that have affected critical infrastructures globally b. Topics include: Presidential Decision Directive – 63, The National Strategy to Secure Cyberspace and an introduction to the National Infrastructure Protection Plan with an overview of the 18 Sectors, and a brief history of cybersecurity incidents of national significance. 2. Technology in Critical infrastructure a. Learning Objectives: At the end of this class, you should be able to: i. Discuss technologies that are deployed across the 18 sectors ii. Understand challenges particular to safeguarding SCADA/PCS iii. Describe the approach taken in the US to safeguard the Internet iv. Explain different strategies for information sharing and cyber incident coordination and response b. Topics include: Technological Challenges, and a focus on Industrial Control Systems, Managing risk to the Internet, Information Sharing and Analysis Centers, WARPs, CERTs. 3. The National Infrastructure Protection Plan (NIPP) a. Learning Objectives: At the end of this class, you should be able to: i. Understand the programmatic structure of the NIPP

ii. Explain the NIPP Risk Management Framework
iii. Describe how the NIPP integrates private industry

b. Topics include: The NIPP Risk Management Framework, The 18 Sectors, Sector Coordinating Councils, Government Coordinating Councils, Cross Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Plans, The role of DHS, private organizations, and other key stakeholders.

4. Cybersecurity in key sectors
   a. Learning Objectives: At the end of this class, you should be able to:
      i. Discuss how the Energy, IT, Communications, and Chemical sectors have approached cybersecurity
      ii. Describe the role of the NERC CIP Standards, and the CFATS standards
   b. Topics include: The Energy Sector, NERC CIP Standards, and DOE cybersecurity efforts, the Information Technology Sector, the Communications Sector, Chemical Facilities Sector and the Chemical Facilities Anti-Terrorism Standards.
5. Current Cybersecurity Challenges in CIP
   a. Learning Objectives: At the end of this class, you should be able to:
      i. Describe recent legislative and regulatory developments in national cybersecuirty
      ii. Describe cybersecuirty, Critical Infrastructure, and cyber weapons
      iii. Explain supply chain challenges and their connection to cybersecurity
      iv. Discuss obstacles to information sharing between private organizations and the government
      v. Recognize critical infrastructure dependencies and interdependencies and associated vulnerabilities
   b. Topics include: Current legislation related to CIP and cybersecurity (Ex. The Cybersecurity Act of 2012) Malware: Stuxnet, DuQu, and Flame, Supply Chain Risk, Information Sharing, Dependencies and Interdependencies.
6. Integrating cyber security management with national cybersecurity
   a. Learning Objectives: At the end of this class, you should be able to:
      i. Understand how a private organization can connects its cybersecurity efforts to its sector and the NIPP
         1. Explain the role of DHS, US-CERT, and ICS-CERT and how these resources might assist a private company.
   b. Topics include: How does an individual integrate CIP? What are operational concerns of cybersecurity managers? How might an organization get assistance from their sector partners and/or DHS?
7. International CIP Efforts
   a. Learning Objectives: At the end of this class, you should be able to:
      i. Describe key attributes of international cybersecuirty agreements
      ii. Explain how Estonia's recent history has shaped its approach to CIP
      iii. Identify similarities in CIP efforts across Asia, Latin America, Europe, and the Middle East

Topics include: International cybersecurity agreements, CIP in Europe, Estonia and Russia, the Middle East, Asia, and Latin America, and The United Nations/ International Telecommunications Union, The International CIIP Handbook

Course/Topical Outline:*

SCHEDULE OF CLASSES & ASSIGNMENTS

Class schedule and assignments are subject to change. Any change will be communicated at least one week prior to its effect. Unless specific page numbers are identified, it is expected that you read the entire document listed.

Date	Topic/Assignments	Required Readings
March 21	Week 1: Course introduction, Enterprise Cybersecurity, Government Cybersecurity, Overview of CIP At the end of this class, you should be able to: • Explain enterprise cybersecurity performance management • Identify US Government Agency cybersecurity efforts and key initiatives Assignment 1 issued	• APT1 pg. 20-26 • PDD-63 • HSPD-7 • PDD-21 • SP-800-55 pg. 9-19 • SSP of your choice (for the assignment)

		• NIPP pg. 1-14
March 28	Week 2: Key CIP Policy Documents, the NIPP, DHS, At the end of this class, you should be able to: • Recognize key policies and salient components regarding cybersecurity and CIP in the US • Understand the challenge of CI asset identification • Critique the NIPP's treatment of cyber security • Identify components of DHS' cybersecurity efforts	• NIPP pg. 27-49, 113-123, 147-157 • EO • NSSC vii – 18 • SSP of your choice continued (for the assignment) • ES-C2M2 pg. 1-3, domain introductions of each domain in the model. • CSTF
April 4	Week 3: The Energy Sector, Public/Private Partnerships and Challenges of Information Sharing At the end of this class, you should be able to: • Relate cybersecurity challenges in the Electricity Subsector • Discuss public perception, expectations, and challenges of cyber information sharing • Identify current legislative initiatives regarding cybersecuirty information sharing • Explain the role of an ISAC, and identify sectors with active ISACs • Evaluate cyber security activities of information sharing organizations	• NSISS • CISPA • BestPractices pg. 4-8 • CSIS2 pg. 1-21 • CIOReportGuide
April 11	Week 4: NCSIRTs, Key Technologies in CIP, intro to cyber exercise At the end of this class, you should be able to: • Identify roles of national computer security incident response teams (NCSIRTs) • Recognize key technologies in CIP • Discuss key cyber events that have impacted policy Assignment #1 Due, Assignment #2 issued	• Exercise Materials (on Bboard)
April 18	Week 5: Cyber Exercise • Cybersecurity Exercise	• GenericFramework • International CIIP pg. 359-369, 421-432
April 25	Week 6: International CIP programs Guest Speaker, please ensure you arrive to class on time. At the end of this class, you should be able to: • Discuss international CIIP efforts • Identify nations who have been working on CIIP programs • Begin (or refine) your responses to Assignment 2	•
May 2	Week 7: How do CIKR Integrate with national efforts? Guest Speaker, please ensure you arrive to class on time. At the end of this class, you should be able to: • Explain how cybersecurity managers in CIKR might align their efforts to national programs Assignment #2 Due	None

Supplemental Reading (not required)

Title	URL
"Critical Path: A Brief History of Critical Infrastructure Protection in the United States" Kathi Ann Brown, © 2006 Spectrum Publishing Group, Fairfax, VA	http://cip.gmu.edu/archive/CIPHS_CriticalPath.pdf
"Cyber Security Strategy" Ministry of Defence, Estonia, Tallinn 2008	http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf
"National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace" ENISA, 2012	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport
"The Comprehensive National Cybersecurity Initiative"	http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

	"ITU National Cybersecurity Strategy Guide"	http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
	"Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada" © 2010 Her Majesty the Queen in Right of Canada	http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf
	"International CIIP Handbook: 2008/2009" E. Brunner, M. Suter, © 2008 Center for Security Studies (CSS), ETH Zurich	http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=91952&lng=en
	The Cybersecurity Act of 2012	http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105
	"RAMCAP ™: The Framework" ASME Innovative Technologies Institute, LLC	http://www.personal.psu.edu/jsd222/SRA311/RAMCAPframework_Risk_Analysis_and_Manage.pdf
	The National Response Framework	http://training.fema.gov/EMIWeb/IS/IS800b.asp

Plagiarism and cheating notice*

ACADEMIC CONDUCT

While you are encouraged to work together and with others in the academic community to further your understanding of the course material, you may not present the work of others as your own. Plagiarism and cheating are serious offenses. Written assignments that contain the work of others without proper citation will automatically receive a failing grade. Further, this offense will be reported to the Dean of the Heinz College so that further disciplinary action can be considered. Plagiarism includes, but is not limited to:

- Presenting another writer's work as your own;
- Cutting and pasting content verbatim without using quotation marks to indicate a direct quote or paraphrasing content without citing the source in-text using parenthetical references, footnotes, or endnotes in addition to listing each source on the Works Cited, References, or Notes page in a manner consistent with the format detailed in an approved style guide (APA or MLA);

Providing incomplete or incorrect information about the source cited.