Syllabus

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

NAME OF SCHOOL:

DEPARTMENT:

PROGRAM:

PROFESSOR:
Telephone Number:
Office Location:
Office Hours:
Email:
Website:

COURSE DESCRIPTION/OVERVIEW:

The 21st century risk environment is a complex mix of manmade and naturally occurring threats and hazards including, but not limited to: international and domestic terrorism, malicious "insiders," active shooters, hurricanes, earthquakes, floods, power outages, hazardous materials spills, industrial accidents, pandemic influenza, malicious cyber intrusions, and climate change. Within this risk environment, our critical infrastructures are inherently vulnerable — domestically and internationally — both within and across sectors due to the nature of their physical attributes, operational environments, international supply chains, and logical interconnections. Hence, the critical infrastructure mission area requires a focused national strategy appropriately balancing resilience — a traditional American strength — with focused, risk-based prevention, protection, and preparedness activities so that we can manage and reduce the most serious risks to the American people and the infrastructures that serve them. Putting this strategy into practice, in turn, requires an unprecedented partnership and information sharing between the public and private sectors at all levels.

This 15-lesson graduate level course provides an introduction to the policy, strategy, and practical application of critical infrastructure security and resilience (CISR) from an all-hazards perspective. It describes the strategic context presented by the 21st century risk environment, and discusses the challenges and opportunities associated with the following: infrastructure- related public-private partnerships; information-sharing; risk analysis and prioritization; risk mitigation; performance measurement; incident management; and

planning and investing for an uncertain future.

This is a multi-faceted course that will expose participants to complex intergovernmental and public-private sector policymaking; risk analysis and management; strategic planning; and crisis management. The course is designed to promote subject-matter understanding, critical analysis of issues, and insight into risk-informed decision-making. It also includes a practical examination of stakeholder interaction and key subject-matter areas through an interactive tabletop exercise (TTX), research paper, and oral presentation. The course promotes a holistic understanding of various approaches to CISR, applicable to the different sectors identified in the National Infrastructure Protection Plan 2013 (NIPP 2013), as well as infrastructure systems which cross national borders or are inherently international in nature.

CREDITS CONFERRED: 3

PREREQUISITE: None

LEARNER OUTCOMES/OBJECTIVES:

This course is designed to enable learners to:

1. Explain the evolution of CISR as a core homeland security policy area:

- The advancement of CISR as a policy focus area, overarching policies and policy approaches, and implications for policy making today
- Executive and Congressional engagement in the CISR mission space
- Real-world incidents as focusing events for policy development and implementation

2. Assess the 21st century risk environment and its application to the CISR mission area:

- Threats: terrorism, cyber-attacks, natural disasters and naturally occurring phenomena, unintentional manmade events, and other emergencies
- Vulnerabilities (facility, node, and system level)
- Consequences (public health and safety, economic loss or disruption, continuity of government/business and essential services, mission degradation, iconic loss, etc.)
- Critical infrastructure dependencies and interdependencies
- Informing executive and managerial decision-making that can reduce risk and increase resilience within and across sectors, regionally, nationally, and internationally

3. Identify and evaluate the roles and responsibilities of key critical infrastructure public and private sector stakeholders:

- Federal; State, local, tribal, territorial (SLTT); regional; and private sector (profit and not-for-profit) stakeholders
- International stakeholders
- Influence of regulations and formal/informal incentives

- Sensitivity to different perspectives and taxonomies

4. Analyze CISR partnership frameworks, information sharing processes and systems, and coordination/collaboration challenges:

- Federal, SLTT, regional, and private sector collaboration, coordination, and communication
- International collaboration
- Critical infrastructure data collection, warehousing, sharing, and protection
- Challenges and opportunities

5. Compare different strategic approaches to and issues regarding critical infrastructure risk management, including: risk analysis, cost-benefit analysis, risk mitigation, and performance measurement (regulatory and non-regulatory):

- Physical security
- Cybersecurity
- Insider threats (including personnel security)
- Systems dependencies/interdependencies
- Jurisdictional considerations
- Sector approaches

6. Recognize the complexities associated with effective and efficient CISR assessment, planning, resource allocation, and program management in a dynamic risk and future operating environment:

- Developing future-oriented goals and objectives, risk management approaches, and plans
- Doing more with less: Achieving CISR in a resource constrained environment
- Planning to meet the demands of the future risk and critical infrastructure operational environments

DELIVERY METHOD:

Course delivery will be through mini-lectures, structured collaborative projects, in-class group activities and exercises, guest speakers, and interactive classroom discussions. The assigned course readings include a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans, and strategies), implementation readings (government products that are responsive or attempt to fulfill the requirements of authoritative documents), and external reviews (U.S. Government Accountability Office, Congressional Research Service, etc.). Participants are expected to familiarize themselves with the assigned topics and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and multiple perspectives.

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 instructor in a timely fashion.

3. The completion of all readings assigned for the course is assumed. Since 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. All cell phones and other electronic devices should be turned off before class begins.

GRADING:

Class Participation	30%
Research Paper	30%
Research Paper Presentation	25%
Incident Management Exercise Point Paper	15%

ACTIVITIES, EXERCISE, AND RESEARCH PROJECTS:

1. Research Paper/Oral Presentation (55% -- combined)

Each learner will prepare a 12-15 page research paper on a CISR issue of their choice (national, regional, SLTT, sector, or international focus). The paper should be completed using the following organizational format: problem statement, background (include key players, authorities, resources, etc.), discussion (presentation of alternatives with the identification of pros and cons for each alternative), and recommendations (including rationale behind their selection). Footnotes and citations should be included at the end of the paper in the proper format for review. The paper should focus on the benefits, drawbacks, and obstacles to the practical application of proposed policy alternatives or other solutions to the problem or issue presented. The recommendations section should clearly describe the rationale for the policy option or other solution of choice. Example research paper topics include, but are not limited to, the following:

- How to promote the adoption and implementation of effective CISR strategies and best practices within a voluntary partnership paradigm
- How to best enable the achievement of one or more of the Joint National Priorities or Call to Action items identified in the NIPP
- How to better foster public-private partnerships and critical infrastructure information sharing among the NIPP partners, both sectorally and regionally
- How to measure the performance of CISR activities within and across sectors and jurisdictions
- How to promote effective critical infrastructure risk mapping as part of the National Preparedness System

- How to best integrate CISR-related priorities into emergent threat and incident response at the SLTT level

As an alternative to a research paper, learners may submit a 12-15 page, section-by-section critique of an existing CISR sector or sub-sector level plan; or a Federal, SLTT, or regional CISR plan or policy. Learner critiques should include alternative visions/strategies for successful CISR program implementation within the sector, agency jurisdiction, or geographic region under study.

Each learner will present his/her research topic or critical analysis (no more than 25-30 minutes in length) to the class during Lessons 13-14. The presentation format will mirror the organizational structure of the research paper or critical analysis completed. **Research papers will be submitted prior to class on Lesson 15. Papers may be submitted electronically.**

Prior approval of the topic for the research paper is required. **Learners should submit a one-paragraph written description of their proposed topic in class or via email for instructor approval no later than the beginning of class on Lesson 5.**

2. Incident Management Exercise (15%)

Learners will participate in a role-based, interactive TTX simulating a complex emergency with major cascading critical infrastructure and population impacts. Two options are presented for this exercise: 1) a terrorist attack scenario, and 2) a hurricane scenario. A complete scenario and discussion modules for each option are provided in Attachments 1 and 2, respectively, to this syllabus. For exercise purposes, each learner will be assigned a role as a key public or private sector official with attendant critical infrastructure concerns and responsibilities. The exercise will include an emerging threat phase, operational response phase, and post-incident recovery phase. In preparation for the exercise, each participant will develop a short paper in talking point format delineating his/her assigned role-based responsibilities, priorities, and challenges corresponding to each phase of exercise play. **This point paper will be submitted at the beginning of class on the day of the classroom exercise.**

3. Expectations for Participation (30%):

Participation includes coming to class prepared, participating in class discussion, and dynamic role playing during the CISR incident management exercise.

INCORPORATION OF FEEDBACK:

The course instructor will offer multiple opportunities for learners to provide constructive feedback 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 complete in-class evaluations at the end of Lesson 6, following the incident management exercise, and at the end of the course. On-line feedback is also encouraged

throughout the course. Finally, the instructor will provide written feedback to learners on the course research paper, oral presentation, and incident management exercise point paper. Ongoing student dialogue with the instructor regarding project development, oral presentation preparation, and incident management exercise preparation is highly encouraged.

COURSE TEXTBOOKS:

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

Lewis, Ted G. (ed.), *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Second Edition, John Wiley & Sons, Inc., 2015.

Collins, Pamela A. and Baggett, Ryan K., *Homeland Security and Critical Infrastructure Protection*, Praeger Security International, 2009.

Brown, Kathi Ann. *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*, Spectrum Publishing Group, 2006.

ARTICLES AND REPORTS:

Various articles and reports are included as required and recommended readings in each individual lesson as identified in the lesson descriptions section below.

ADDITIONAL RESOURCES (UNRESTRICTED PUBLIC ACCESS):

Critical Infrastructure Resource Center:
http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/index.htm

U.S. Department of Homeland Security Office of Infrastructure Protection:
http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm

U.S. Department of Homeland Security Daily Open Source Infrastructure Report:
http://www.dhs.gov/files/programs/editorial_0542.shtm

Emergency Management Institute Independent Study Program:
http://training.fema.gov/IS/

Homeland Security Digital Library:
http://www.hsdl.org/

The CIP Report:
http://cip.gmu.edu/the-cip-report

ADDITIONAL RESOURCES (SUBSCRIPTION REQUIRED):

Administrative Note: The resources identified below can be accessed via the following procedure – (TBD based on individual school policy).

The International Journal of Critical Infrastructures:
http://www.inderscience.com/browse/index.php?journalID=58

Homeland Security Affairs:
http://www.hsaj.org/

The Journal of Homeland Security and Emergency Management:
http://www.bepress.com/jhsem/

The Journal of Homeland Security:
http://www.homelandsecurity.org/journal/Default.aspx

The Journal of Homeland Security Education:
www.JournalHSE.org

The European Journal of Transport and Infrastructure Research:
http://www.tbm.tudelft.nl/index.php?id=105305

The International Journal of Sustainable Transportation:
http://www.tandf.co.uk/journals/titles/15568318.asp

The Journal of Transportation Law, Logistics & Policy:
http://www.atlp.org/index.php?option=com_content&view=article&id=12:journal-of-transportation-law-logistics-policy&catid=9&Itemid=116

The International Journal of Logistics Management:
http://www.emeraldinsight.com/journal/ijlm

The International Journal of Electrical Power & Energy Systems:
http://www.journals.elsevier.com/international-journal-of-electrical-power-and-energy-systems/

The Global Homeland Security Education Network:
http://www.northumbria.ac.uk/sd/academic/sass/about/socscience/solscres/interdiscnetworks/ghsen/

GRADING SCALE (SCHOOL POLICY DEPENDENT):