Introduction to Critical Infrastructure Protection
(CRIM 3460 Section 201)
Spring 2016
School of Criminology and Justice Studies
Monday and Wednesday 12:30 – 1:45 PM
Coburn Hall, Room 210

Instructor: Gary Gordon, P.E.
Email: Gary_Gordon@uml.edu
Office Hours: Before and after class, and by appointment
Course Website: http://faculty.uml.edu/Gary_Gordon/

Required Textbook


Supplemental Reading


Moteff, John (2015), Critical Infrastructures: Background, Policy, and Implementation, Congressional Research Service

Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts, Governmental Accountability Office, 2014

Relevant Links


Critical Infrastructure and Key Resources Support Annex: http://www.dhs.gov/critical-infrastructure-and-key-resources-support-annex


HSPD 7: http://www.dhs.gov/homeland-security-presidential-directive-7
Course Description

This course provides an introduction to one of the most important aspects of homeland security: critical infrastructure and the protection thereof. In the course, the student will be introduced to the concept and components of the country’s critical assets and threat environment; federal government plans and how public-private partnership protection efforts are leveraged; and strategies and methods of protecting critical infrastructure. This course will culminate in a discussion of critical infrastructure security threats, vulnerabilities and risks; and how it protects and hardens itself from threats. Case studies will be used so that the student can understand how the principles and processes of infrastructure protection apply to “real world” situations and solutions.

Course Objectives

The following are the objectives for the course to provide the student with an understanding of the various components and relationships of critical infrastructure protection. These objectives will be reviewed and refined, as needed, to reflect the material presented.

- The origins of homeland security and critical infrastructure protection.
- Government’s role in critical infrastructure protection.
- The challenges and trade-offs in protecting critical infrastructure.
- The principles of risk and associated strategies, and relationship to catastrophic events.
- Critical infrastructure security threats, vulnerabilities and risks.
- The importance Critical Infrastructure Key Resources (CIKR).
- The sectors comprising critical infrastructure, characteristics and relationships.
- The value of studying lessons learned regarding critical infrastructure protection from a multidisciplinary perspective.
- The consequences of compromising critical infrastructure.
- When critical infrastructure is to be protected and/or hardened and how accomplished.
- The principles of system redundancy in critical infrastructure protection.
- The methods of protecting critical infrastructure and providing system redundancy.
- The relationship between the government and the private sector in critical infrastructure protection.

Course Outcomes

Upon completion of the course, the student should be able to understand the: origins of homeland security and critical infrastructure protection; government’s role; relationship between the government and the private sector; social and economic challenges and trade-offs; principles of risk and associated strategies; security threats, vulnerabilities and risks; significance of Critical Infrastructure Key Resources (CIKR); individual sectors and their characteristics and relationships; value of studying lessons learned; consequences of compromising critical infrastructure and when critical infrastructure is to be protected and/or hardened and how it can be accomplished; principles of system redundancy; and different methods of protecting critical infrastructure and providing system redundancy. Also, the student should be familiar with analytical methods used in critical infrastructure protection analysis and various Department of Homeland Security (DHS) organizations and programs facilitating critical infrastructure protection.
Teaching Methods

The class will be in lecture and discussion format, and will be presented through the use of PowerPoint presentations and select videos. Guided in-class work and independent assignments from outside sources will also be used.

Course Requirements and Instructor Expectations

Students are expected to attend class prepared; meaning, at a minimum, that they have read the assignment for that day’s class. All assignments will be related to the textbook, lectures and discussions held in class, and readings and other work, as assigned. All material will be either handed out in class or provided via the course website. I will present the course material, raise questions, lead discussions and assist in the interactive learning of the class. Students will be required to actively participate during class to the maximum extent possible, and will be expected to discuss topical and current media articles and issues germane to the class and to initiate class discussion. The student is responsible for all material covered during this course. If you are to be absent due to illness or other extenuating circumstances, you should contact me, in advance, about making up the work you missed.

Participation

"Qualitative points” to the professionalism grade for the course will be given by the instructor based on the student’s level of participation during the course.

Attendance

Class attendance and participation are integral to the learning process. Perfect attendance is expected, however, each student will be allowed three unexcused (3) absences to cover such things as illnesses, jury duty, family emergencies, military duty, etc. Attendance will be taken for each class. See the “Professionalism” section for further information.

Exams

There will be three (3) in-class exams and a final examination conducted during the semester. There will also be four (4) FEMA Emergency Management Institute (EMI) Independent Study Program (ISP) courses assigned during the semester, which will count as a fourth exam. See the section below on the FEMA EMI ISP courses.

- The in-class exams will include material covered during a given period and subsequent to a previous exam (i.e. Exam #2 will cover material subsequent to that covered in Exam #1).
- The Final Exam will include all material covered during the semester.
- Exams will consist of multiple choice, true/false and short essay questions.
- All Exams will include extra credit questions taken from class discussions and readings.
- Since the FEMA EMI ISP courses are pass/fail, they will be graded in the following manner:
<table>
<thead>
<tr>
<th>FEMA EMI Submissions</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit one ISP course on time</td>
<td>60</td>
</tr>
<tr>
<td>Submit two ISP courses on time</td>
<td>70</td>
</tr>
<tr>
<td>Submit three ISP courses on time</td>
<td>85</td>
</tr>
<tr>
<td>Submit all fours ISP courses on time</td>
<td>100</td>
</tr>
<tr>
<td>Late submission of an ISP course</td>
<td>5 grade point deduction per each late submittal</td>
</tr>
</tbody>
</table>

*Note: ISP courses will not be accepted after five (5) days after the due date.*

**Semester Project/CIS Analysis**

A Critical Infrastructure Sector (CIS) Analysis project will be required during the semester. It will be a scholarly research paper and accompanying presentation that exhibits the students’ knowledge gained from the text, other material provided and independent research on a “real world” conditions involving critical infrastructure. The CIS Analysis will be a group effort to conduct an industry specific security review of one of the sixteen (16) critical infrastructure sectors. The research paper will include a class presentation that summarizes the research and addresses the characteristics of the sector; threats, vulnerabilities, consequences and risks involved; and mitigation measures to reduce the risk and minimize the impacts. Details of the assignment will be provided in a separate document early in the semester outlining the requirements and submittal dates, and will be posted on the class website.

**FEMA Emergency Management Institute (EMI) Independent Study Program (ISP) Courses**

The FEMA EMI ISP has a series of courses that relate to critical infrastructure and resilience and are the foundation of its Critical Infrastructure Security and Resilience series. These courses build upon what is covered in the textbook and show how FEMA and industry address critical infrastructure and key resources. There are four (4) foundation courses in the series that link critical infrastructure protection and disaster mitigation. These independent study courses average two (2) hours each and will be assigned during the semester to familiarize the student with the role critical infrastructure protection and resilience plays in emergency management, preparedness planning, response and recovery. Details of the assignment will be provided in a separate document early in the semester outlining the requirements and submittal dates, and will be posted on the class website.

**Professionalism**

Each student will start the semester with 100 “professionalism” points and will lose points for being “unprofessional”, as listed below. Student will lose points as follows:

- Absences greater than 3 (4 point deduction per absence)
- Late submission of work (3 point deduction for each calendar day. Deliverables will not be accepted after 5 days.)
- Missed test without prior arrangement with instructor (10 point deduction for each)
- Late for office hours appointment with instructor (2 point deduction for each)
- Missed office hours appointment with instructor (4 point deduction for each)
- Instructor discretion (1-10 points)

Students with perfect attendance for the semester will receive 5 bonus points added to the professionalism grade.
Assignment and Exam Grading Breakdown

<table>
<thead>
<tr>
<th>Graded Assignment</th>
<th>Percent of Final Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEMA EMI ISP Courses/Exam</td>
<td>10%</td>
</tr>
<tr>
<td>Exams</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
<tr>
<td>Group Project</td>
<td>30%</td>
</tr>
<tr>
<td>Professionalism</td>
<td>20%</td>
</tr>
</tbody>
</table>

Grading is as follows:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Grade Point</th>
<th>Grade Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>4.0</td>
<td>95% - 100%</td>
</tr>
<tr>
<td>A-</td>
<td>3.7</td>
<td>90% - 94%</td>
</tr>
<tr>
<td>B+</td>
<td>3.3</td>
<td>87% - 89%</td>
</tr>
<tr>
<td>B</td>
<td>3.0</td>
<td>83% - 86%</td>
</tr>
<tr>
<td>B-</td>
<td>2.7</td>
<td>80% - 82%</td>
</tr>
<tr>
<td>C+</td>
<td>2.3</td>
<td>77% - 79%</td>
</tr>
<tr>
<td>C</td>
<td>2.0</td>
<td>73% - 76%</td>
</tr>
<tr>
<td>C-</td>
<td>2.7</td>
<td>70% - 72%</td>
</tr>
<tr>
<td>D+</td>
<td>2.3</td>
<td>65% - 69%</td>
</tr>
<tr>
<td>D</td>
<td>1.0</td>
<td>60% - 64%</td>
</tr>
<tr>
<td>F</td>
<td>0.0</td>
<td>59% and below</td>
</tr>
</tbody>
</table>

Email

The university’s e-mail system should be used for one-on-one correspondence and for reminders and general announcements to the entire class. Therefore, it is important that you check your university email account daily (or as often as possible) so that you will not miss any important information. I usually check e-mail in the morning and evening. I will make every effort to respond to all emails within 24 hours of receipt. Please make every attempt to use email for matters dealing with private or personal issues, and include your full name and course number, name and section. Questions related to the course material should be in class, as any answers or further discussion may benefit the class as a whole.

Expectations of Student Behavior in the Classroom

Students are expected to exhibit professional and respectful behavior that is conducive to a mutually beneficial learning environment in the classroom. Examples of inappropriate behavior include, but are not limited to:

- Text messaging
- Listening to music
- Cell phone use (other than for the campus alert system)
- Late arrivals/early departures (without prior arrangement)
- Use of laptops/iPads/other electronic devices for other than class purposes
- Sleeping in class
- Disrespectful comments or behavior
• Intentional disruptions
• Failure to follow faculty directives.

Exceptions to these behaviors would only be granted with the permission of the faculty. Students that violate these standards will, at the very least, have their professionalism grade affected or may be asked to leave the class and/or be referred to the Dean of Students for disciplinary action.

**Academic Honesty**

There are many definitions for academic dishonesty; cheating and plagiarism are two. Cheating is defined as dishonesty of any kind in connection with assignments and examinations. This applies to both giving and receiving unauthorized help or answers. Plagiarism is defined as presenting the work of someone else as one’s own. Cheating and plagiarism include, but are not limited to:

• Using any unauthorized aids on an exam or test
• Representing or submitting someone else’s work as your own
• Falsifying documents or grades
• Submitting the same essay or report in more than one course (without permission)
• Looking at someone else’s answers during an examination
• Impersonating another person or having someone impersonate you when taking an exam
• Making up sources or facts for an essay or report

Unless specified otherwise, your work must be yours and yours alone. Collaboration will be permitted on certain and/or a group assignments. When you use the work of others, whether out of books, journals, websites, spoken word or from any other media source, that work must be credited and properly annotated.

• Using sources to broaden your knowledge, to inform your ideas, to help build the case for your positions, is an expected component of scholarship. Substituting others’ ideas for your own analysis is not acceptable.

Any infraction of the University’s Academic Honesty Policy may take the form of the following academic sanctions:

• Failure on the assignment in question
• Failing grade for the course. Note that a failing grade will take precedence over any attempt to withdraw from the course.
• Notification of the University of the misconduct of the student
• Recommendations that the student be suspended or dismissed from the University
<table>
<thead>
<tr>
<th>Week</th>
<th>Dates</th>
<th>Assignment</th>
<th>Covered Material and Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jan. 20 (Wed)</td>
<td>Read Ch. 1</td>
<td><em>Origins of Critical Infrastructure Protection</em></td>
</tr>
<tr>
<td>2</td>
<td>Jan. 25 (Mon) Jan. 27 (Wed)</td>
<td>Read Ch. 2 Read Ch. 3</td>
<td><em>Risk Strategies Theories of Catastrophe</em></td>
</tr>
<tr>
<td>3</td>
<td>Feb. 1 (Mon) Feb. 3 (Wed) <em>Read Ch. 7</em></td>
<td>Security Vulnerability Assessment FEMA EMI IS-821.a or approved alternate (Wed) CIP Analysis paper team and sector proposal due (Wed)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Feb. 8 (Mon) Feb. 10 (Wed)</td>
<td>Read Ch. 4</td>
<td><em>Complete CIKR Systems</em> FEMA EMI IS-860.b or approved alternate (Wed)</td>
</tr>
<tr>
<td>5</td>
<td>Feb. 16 (Tues) Feb. 17 (Wed)</td>
<td>Read Ch. 5</td>
<td><em>Communications</em> FEMA EMI IS-913.a or approved alternate (Wed) Exam #1 (Wed) Chapters 1 - 4</td>
</tr>
<tr>
<td>6</td>
<td>Feb. 22 (Mon) Feb. 24 (Wed)</td>
<td>Read Ch. 6 Read Ch. 7</td>
<td><em>Internet Cyber Threats</em> CIP Analysis paper abstracts and outlines due (Mon) FEMA EMI IS-921.a or approved alternate (Wed)</td>
</tr>
<tr>
<td>7</td>
<td>Feb. 29 (Mon) Mar. 2 (Wed) Read Ch. 8 Read Ch. 9</td>
<td>Information Technology Cybersecurity Policy</td>
<td>Independent work on CIP Analysis papers (Mon)</td>
</tr>
<tr>
<td>8</td>
<td>Mar. 7 (Mon) Mar. 9 (Wed)</td>
<td>Read Ch. 10</td>
<td>Supervisory Control and Data Acquisition Tour of USCG District 1, Boston (Fri) in lieu of 3/2 class</td>
</tr>
<tr>
<td></td>
<td>Mar. 14 – 18 Spring Recess</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Mar. 21 (Mon) Mar. 23 (Wed)</td>
<td>Read Ch. 11</td>
<td><em>Water and Water Treatment</em></td>
</tr>
<tr>
<td>10</td>
<td>Mar. 28 (Mon) Mar. 30 (Wed)</td>
<td>Read Ch. 12 Read Ch. 13</td>
<td>Energy Electric Power Exam #2 (Wed) Chapters 5 – 10</td>
</tr>
<tr>
<td>11</td>
<td>Apr. 4 (Mon) Apr. 6 (Wed)</td>
<td>Read Ch. 15</td>
<td>Transportation Independent work on CIP Analysis (Mon) Draft CIP Analysis papers due (Wed)</td>
</tr>
<tr>
<td>12</td>
<td>Apr. 11 (Mon) Apr. 13 (Wed)</td>
<td>Read Ch. 16</td>
<td>Supply Chains Independent work on CIP Analysis papers/presentations (Wed)</td>
</tr>
<tr>
<td>13</td>
<td>Apr. 20 (Wed) Apr. 22 (Fri)</td>
<td>Read Ch. 14 Read Ch. 17</td>
<td>Healthcare and Public Health Banking and Finance Exam #3 (Mon) Chapters 11 – 13, 15 and 16 Final CIP Analysis papers due (Wed)</td>
</tr>
<tr>
<td>14</td>
<td>Apr. 25 (Mon) Apr. 27 (Wed)</td>
<td></td>
<td>CIP Analysis presentations</td>
</tr>
</tbody>
</table>

Note: The course schedule is tentative and subject to change, which will be announced in class or via UML e-mail with as much notice as possible. Students are responsible for being aware of any changes.