Goals & Objectives
Ensuring the security and resilience of the critical infrastructure/key resources of the United States is essential to the Nation’s security, public health and safety, economic vitality, and way of life. To meet this requirement, H SEC 690 – Critical Infrastructure and Key Resources Protection has been designed as a 3-unit graduate seminar, comprised of in-depth analysis of critical infrastructure and key resources identification and protection strategies, discussion and application of risk identification and evaluation, risk assessment modeling, threat identification and briefing practicum, origin, storage, and use, of Protected Critical Infrastructure Information (PCII), and exploration of government and private sector roles, responsibilities, authority and policy concerning critical infrastructure and key resources.

Graduate Program in Homeland Security Goals:
The mission of the Graduate Program in Homeland Security is to produce leaders from a variety of educational and professional backgrounds who can effectively and efficiently identify, design, and mobilize the appropriate community resources to identify, prevent, deter, preempt, defend against, and respond to terrorist attacks and/or other critical incidents and emergencies on the local, regional, national and international levels.

H SEC 690 contributes to these goals through its student learning outcomes . . .
1. Define critical infrastructure and key resource systems and services, and the importance they play in the national and global economy and quality of everyday life.
2. Define common terms associated with infrastructure operation and protection such as threat, risk, reliability, robustness, redundancy, and resiliency.
3. Interpret and discuss national, state, local, tribal and territorial (SLTT) strategy and policy documents related to the authority of both government and the private sector to manage and protect critical infrastructure and key resources, and the sensitive information about them.
4. Comprehend the operation of critical infrastructure and key resources (i.e. transportation, electricity, water) and understand their interwoven dependencies, potential susceptibility for failure, and consequences of their failure to function normally.
5. Develop and deliver management-level threat intelligence and situational awareness briefings on specific critical infrastructure and key resource sectors.
6. Evaluate and apply solutions to prevent and respond to failures in complex infrastructure systems.
7. Analyze the United States government’s approach to critical infrastructure and key resource assurance, to those used by other nations, and the private sector.
8. Synthesize threat and risk information into a threat and vulnerability assessment model to measure acceptable risk levels, and choose appropriate and feasible risk mitigation strategies.
3. **Topics to be covered**

- **Unit 1:** Introduction to Critical Infrastructure and Key Resources  
  2 Weeks
- **Unit 2:** Government and Private Sector CIKR Authority and Roles  
  1 Weeks
- **Unit 3:** Threats and Hazards to Infrastructure  
  1 Weeks
- **Unit 4:** Vulnerability and Risk  
  1 Weeks
- **Unit 5:** Risk Assessment/Management Strategies  
  1 Weeks
- **Unit 6:** The Role of Threat Intelligence  
  2 Weeks
- **Unit 7:** National Infrastructure Protection Plan  
  1 Weeks
- **Unit 8:** Critical Infrastructure Design and Operation  
  1 Weeks
- **Unit 9:** Managing Incidents: Incident Command System  
  2 Weeks
- **Unit 10:** Case Studies  
  1 Weeks
- **Unit 11:** Student Risk Assessment Presentations  
  1 Weeks

4. **Course Design**

To effectively realize the learning objectives and outcomes, this course relies on various pedagogical approaches: reading assignments, classroom lectures, critical discussions, student briefings, projects, and other hands-on assignments. The reading assignments are an important self-learning tool and the classroom lecture is designed to supplement the reading assignment by clarifying and elaborating challenging concepts. H SEC 690 is a seminar course on critical infrastructure and key resources, therefore, during the lecture, the instructor will be assuming students will participate actively in discussion and critical thinking. Students should not hesitate to question seemingly common knowledge, and discuss controversial topics in an open and non-judgmental educational environment.

5. **Instructor Availability**

In-class is the best medium for answering questions about course content, as the answer benefits the entire class. It is, however, the goal of the course instructor to be available outside of class to answer any questions about course schedule, policy or to discuss extenuating circumstances. The best way to reach your instructor is by email. E-mail is checked often, but you may also telephone your instructor at the phone number above. Office hours are also available at the times listed above.

6. **Required Textbook & Reference Sources**

- This is a course reader which is available from the SDSU Bookstore beginning Monday August 25th, 2014. The price will be $10.63.

7. **Conduct in Class**

As a graduate-level course, your attendance at each class meeting is required. Students are expected to be prepared for all class meetings. Class lectures will not simply cover material available through the readings. If you are absent or not prepared, your learning will be negatively affected. If you are unavailable due to work or another event, you are still responsible for any work assigned or discussed in class. Please let the instructor know if you will be missing a class due to a foreseeable or unforeseeable absence. Team up with several other students to have a resource for in-class information you might miss. Attendance is not part of the points that make up your class grade, but I guarantee you, your grade will directly reflect your level of attendance and participation.

8. **Classroom Courtesy is Required**

Disrespectful and/or disruptive behavior will result in removal from class and/or loss of course points. Newspaper reading, using a cell phone or headphones, doing work for other classes or employment, talking during class, and sleeping are a few examples of activities that will be considered disrespectful and/or disruptive. Additionally, you should arrive to class on time and leave when the course is adjourned. If you bring food or drink to class, please do not leave your trash/mess for others to clean up. Text Messaging during a lecture is discourteous. You will be asked to leave class if you use your phone during class time. If you need to take a phone call or send a message, feel free to do
so outside the classroom. You will not distract the instructor if you silently exit the classroom to take a quick break or phone call.

9. General Class Policies
- Course information including the syllabus, assignments and scores will be updated on Blackboard. Students are required to check Blackboard on a regular basis to keep informed of updates, especially any class schedule changes.
- All students should turn off their cell phones and laptop computers during the class to avoid distraction. Sometimes a laptop can be a good tool for additional research while class is in session. However, if you are gaming, messaging friends, visiting social media sites, or doing other non-academic or research activities on your laptop, you are being discourteous to fellow students and your instructor, and you will be asked to leave.
- Please be punctual. Being late is a disrespectful behavior to the instructor and classmates.
- Academic dishonesty is against University rules and regulation. Students caught giving or receiving assistance to/from another student(s) during any non-group assignments will be asked to leave and will receive an F for the course. Every case will be reported to the Center for Student Rights and Responsibilities for possible disciplinary action. Visit http://www.sa.sdsu.edu/srr/index.html for more information on academic dishonesty.

10. Exam and Grading Policies

Certification Exams
- Students will use the Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI) Independent Study Program (ISP) located at http://training.fema.gov/IS to complete several certification exams involving critical infrastructure and key resources during the course. The courses are open and free of charge to any U.S. citizen. See the course schedule below for specific exam assignments and due dates. If you are an international student without a social security number, you must be sponsored by both the instructor and the University to use the system. Please see the instructor during the first day of the course if you are a student in this category.
- The FEMA EMI ISP system is web-based and requires a web-browser and internet-connected computer system. If you need further instructions for using the FEMA EMI ISP system or to see the full list of offered courses please visit http://training.fema.gov/IS/docs/IS%20Brochure.pdf.
- You can take each certification exam as many times as necessary to pass. The approximate completion time estimate for each certification course is listed in the course schedule below. Make sure to pay special attention to any courses with a larger amount of time required for completion, so you may adequately prepare.
- Most FEMA EMI ISP certification courses/exams require a 75% pass rate to receive a certificate. You must pass the certification exam and print a certificate of completion for each course completed, and turn this into the instructor, in class, on the certification due date listed in the syllabus. It may take the FEMA system up to 24 hours to deliver your certificate of completion via email, so please plan accordingly. The instructor will allow a one-time grace period for up to one week, from the certification due date listed on the syllabus, to accommodate for any one-time technical issues. After this grace period, you will receive a 0 for the particular certification course grade.
- You may turn-in any certification exam certificate into your instructor earlier than the assigned date without penalty.
- You may select one certification exam grade to “exempt”, without a grade penalty. The instructor recommends using this one-time completion grade exemption for an unforeseeable emergency during the semester, or a certification exam you cannot seem to pass.

List of Assigned Certification Examinations
IS-5.A: An Introduction to Hazardous Materials (10 hours)
IS-100.B: Introduction to Incident Command System, ICS-100 (3 hours)
IS-106.14: Workplace Violence Awareness Training 2014 (1 hour)
IS-156: Building Design for Homeland Security for Continuity of Operations (8 hours)
IS-395: FEMA Risk Assessment Database (2 hours)
IS-454: Fundamentals of Risk Management (2 hours)
IS-821.a, Critical Infrastructure and Key Resources Support Annex (1 hour)
Readings
The majority of assigned readings in this course are contained within the H SEC 690 course reader. Completion and comprehension of the assigned readings is imperative in order for students to adequately contribute to class discussion. Students should leave ample time to complete reading assignments. Students should start working on each assignment early rather than waiting until the last moment because there will be unexpected problems. Sending a frantic last-minute email to your instructor is not good time management, and may not be answered in time to assist you in completing the assignment (start your assignments earlier rather than later).

Project
During the semester, student groups will conduct a Risk Assessment of a publicly-accessible on-campus facility using the Department of Homeland Security, FEMA 452: Risk Assessment Database Assessment Tool. The installation files for the risk assessment tool are located at: https://s3-us-gov-west-1.amazonaws.com/dam-production/uploads/20130726-2112-31471-2521/452_455_database_installation.zip. The purpose of the semester project is to help students understand how to conduct a risk assessment using a risk measurement model, and how risk, vulnerability, exploitation, reliability, robustness, redundancy and resiliency influence critical infrastructure and key resources protection decisions. Please see the course schedule for specific project assignment start and due dates.

Below is a list of safety rules that must be followed during the risk assessment project exercise:

- Do not violate the law or participate in activities that may generate reports of suspicious activity.
- Do not perform any activities that would violate University moral or ethical policy.
- Do not access any non-public spaces, rooms, or locations within and/or outside any building or other type of prohibited location. A good rule of thumb: “if you feel you shouldn’t be there, you shouldn’t be!”
- Perform project activities during normal business hours, and in safe conditions.
- Operate only in the open-source information space. Do not obtain any information that may be considered Protected Critical Infrastructure Information (PCI). If you inadvertently receive PCI information, notify your instructor immediately, and protect the information per PCI standards and requirements.

Daily Threat Briefings
Intelligence, especially threat intelligence, is critical in implementing safeguards or countermeasures to protect critical infrastructure and key resources. In other words, “Forewarned is Forearmed”. Students will deliver a sector-specific threat briefing at the beginning of each class. On the first day of class students will be assigned to a critical infrastructure and key resource sector-specific group with up to two other students. An effort will be made to assign students to critical infrastructure and key resource sector-specific groups they have interest in.

A daily class threat briefing template Word document is available on Blackboard to help organize the daily threat briefing for student groups. The template should be completed before class, and brought to class in paper form. The template does not have to contain a briefing “word-for-word” – so notes or summaries are adequate. The daily threat briefing should be under 3 minutes total, and should include the “critical threat information” from a student group’s specific critical infrastructure and key resource sector, which occurred during the previous week. Only one person from your group should be tasked with presenting each class. The reason for multiple group members is to account for any student absences, so each sector will always be briefed during each class period. Since not all class members can
become “experts” in each of the 16 CIKR sectors during the semester, this exercise is as much for your classmates, as for yourselves.

Students may find information for their daily threat briefing from any open-source. This may include websites such as Google News, CNN, MSNBC, FEMA, DHS. Another good strategy is to setup news or sector-specific keyword alerts on these websites, or directly on a search engine.

**Grading**

Your semester grade will be based on a percentage = (points earned/points possible).

<table>
<thead>
<tr>
<th>ASSIGNMENT &amp; EXAMS</th>
<th>GRADING METHODOLOGY</th>
<th>QUANTITY</th>
<th>UNIT POINTS</th>
<th>TOTAL POSSIBLE POINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Participation</td>
<td>Points – Discretion of Instructor</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Daily Sector Briefing</td>
<td>Points – Discretion of Instructor</td>
<td>14</td>
<td>5</td>
<td>70</td>
</tr>
<tr>
<td>Certification Courses</td>
<td>Credit/no credit (One grade exempt)</td>
<td>12</td>
<td>10</td>
<td>120</td>
</tr>
<tr>
<td>Risk Assessment Project</td>
<td>Points – Discretion of Instructor</td>
<td>1</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL</strong></td>
<td></td>
<td></td>
<td><strong>300</strong></td>
</tr>
</tbody>
</table>

11. **Policy on Incompletes**

Per University policy, an incomplete will only be considered in those cases where a student has completed a significant majority of the course and encounters a justifiable and unforeseen circumstance that prevents him or her from finishing the coursework during the regular semester (e.g., a severe personal emergency late in the semester, substantiated with a doctor’s note, and at the discretion of the professor). The 2014-2015 SDSU General Catalog, under the section University Policies, states that, “An Incomplete shall not be assigned when the only way you could make up the work would be to attend a major portion of the class when it is next offered.” More information is available on page 462 of the general catalog, which is accessible online.

12. **Disability Accommodation**

Students who need accommodation of their disabilities should contact me privately, to discuss specific accommodations for which they have received authorization. If you need accommodation due to a disability, but have not registered with Student Disability Services at 619-594-6473 (Calpulli Center, Suite 3101), please do so before making an appointment to see me.

13. **Changes**

This syllabus is preliminary, and may be changed as needed at the discretion of the Professor. Blackboard is the only designated communications channel for notifying students of any changes or updates to course content, cancelled classes, announcements, or requirements.
14. Non-Attribution Policy

This course (and the Homeland Security degree program) presents the student with a wide range of highly qualified and informative classmates, guest speakers, and instructors. To allow these individuals to speak candidly, they are assured that what is said in lecture, posted on the course website, or mentioned in other electronic, written, or verbal methods, will not be attributed to them outside the classroom, regardless of classification, disclaimer, or public domain. Quoting someone outside the course environment without permission may risk your reputation, or the reputation of others. This most certainly would have the effect of stifling participation, causing them to speak in a guarded manner. Ultimately the quality of education provided would suffer. Hence, what your fellow students, guest speakers, and instructors say during their lectures is not for attribution. It may be acceptable to say “someone in my class” made a particular statement, but the individual’s name will not be divulged. Use good judgment, common sense, morals and ethics when making this determination. Individuals who violate this non-attribution policy are subject to administrative and disciplinary action per University policy.

15. Non-Disclosure Policy

During certain presentations, discussions, or guest lectures, the instructors, guest lecturer, or fellow classmates may ask for discretion on a particular topic. The topic may not be for public distribution or the speaker is simply uncomfortable with its contents being discussed outside the classroom. In order to foster trust and open communication within our classroom, it is strictly required of anyone enrolled or involved in this course to maintain the secrecy of information properly identified as sensitive for a period of no less than five years or until such information enters the public domain or is otherwise released by its originator. Communication within class or on the course website is considered to be "not for disclosure" only if properly identified by the originator by explicit notification. For example, in an online posting that is not for disclosure, its originator should place a disclaimer before the text of a form similar to "NOT FOR PUBLIC DISCLOSURE", or "DO NOT FORWARD". In verbal class discussions, a speaker can indicate a sensitive topic with a statement such as "the following should not leave this room" or similar admonition. Individuals who violate this non-disclosure policy are subject to administrative and disciplinary action per University policy.


Some students, classmates, instructors, guest lecturers, or observers may be under the restrictions of certain U.S. Government Security Clearances issued by the Dept. of Defense, Dept. of Energy, Dept. of State, or other government agencies. Those that hold these security levels must at all times remember their duty to uphold secrecy and must not at any time disclose any information that contradicts oaths, agreements, or pledges of secrecy that they have previously sworn or agreed to. At no point should there be a situation where a student or other class participant mentions during a discussion "Well, this is classified information, but just don’t tell anyone..." or similar situations. The previous non-disclosure policies will not protect an individual that has knowingly violated their secrecy oaths and it is highly recommended that those with sensitive government clearances review the guidelines on information disclosure with their privacy officer and/or facility's security officer.

For the protection of those that hold security clearances, please do not discuss or post online materials which you know or suspect to be under U.S. Government classification. Security clearances prohibit the handling or transmission of documents which exceed the classification level of the individual, or which are displayed outside of approved facilities or information mediums. While you may not be under such restrictions, your classmates could be; your actions can have a detrimental effect on their ability to uphold their oaths, agreements, pledges, or could result in the ineligibility of your classmates to obtain or maintain a security clearance. When in doubt, please consult the instructor prior to discussion in class or online.

17. No Recording Policy

Audio and/or visual recording of any instructor, classmate, or guest lecturer is strictly forbidden, aside from disabilities that require the use of amplification or other recording devices. This course is intended to foster free discussion and recording devices produce a chilling effect on participation.
18. Class Schedule/Reading Assignments

### MIS687 2014 Fall COURSE SCHEDULE

<table>
<thead>
<tr>
<th>Date</th>
<th>Topics, Reading &amp; Research</th>
<th>Reading &amp; Assignments Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 26</td>
<td>Introduction to the Course</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reader: The White House: PPD-21 Critical Infrastructure Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certification: IS-821.a, Critical Infrastructure and Key Resources Support Annex (1 hour)</td>
</tr>
<tr>
<td>Sep 2</td>
<td>Introduction to Critical Infrastructure and Key Resources</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reader: The White House: PPD-21 Critical Infrastructure Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certification: IS-821.a, Critical Infrastructure and Key Resources Support Annex (1 hour)</td>
</tr>
<tr>
<td>Sep 9</td>
<td>Introduction to Critical Infrastructure and Key Resources</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Speaker – Energy Sector</td>
</tr>
<tr>
<td>Sep 16</td>
<td>Government and Private Sector CIKR Authority and Roles</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Speaker - DOJ</td>
</tr>
<tr>
<td>Sep 23</td>
<td>Threats and Hazards to Infrastructure</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Speaker – Government Facilities/CSU</td>
</tr>
<tr>
<td>Sep 30</td>
<td>Class Does Not Meet – Academic Conference – Please Complete your Assignments/Readings</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td>Oct 7</td>
<td>Vulnerability and Risk Risk Assessment/Management Strategies</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Speaker – DHS Protective Security Advisor</td>
</tr>
<tr>
<td>Oct 14</td>
<td>The Role of Threat Intelligence</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Speaker – DHS Cyber</td>
</tr>
<tr>
<td>Oct 21</td>
<td>The Role of Threat Intelligence</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Speaker – DHS Intel</td>
</tr>
<tr>
<td>Oct 28</td>
<td>National Infrastructure Protection Plan</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Speaker – Fusion Center</td>
</tr>
</tbody>
</table>
|        |                                                                                         | Reader: “NIPP 2013: Partnering for Critical Infrastructure - Security and Resilience”    | (pgs1-26)
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 4</td>
<td>Critical Infrastructure Design and Operation</td>
<td>Daily Sector Briefing, Certification: IS-860.b, National Infrastructure Protection Plan (2 hours)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certification: IS-106.14: Workplace Violence Awareness Training 2014 (1 hour)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certification: IS-921.a Implementing Critical Infrastructure Security and Resilience (3 hours)</td>
</tr>
<tr>
<td>Nov 18</td>
<td>Managing Incidents: Incident Command System</td>
<td>Daily Sector Briefing, Certification: IS-100.B: Introduction to Incident Command System, ICS-100 (3 hours)</td>
</tr>
<tr>
<td>Dec 2</td>
<td>Case Studies</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td>Dec 9</td>
<td>Class Wrap-up and In-Class Project Time</td>
<td>Daily Sector Briefing</td>
</tr>
<tr>
<td>Dec 16</td>
<td>Student Risk Assessment Presentations</td>
<td>Project Due: Sector-Specific Campus Risk Assessment Using FEMA 452 Assessment Tool</td>
</tr>
</tbody>
</table>

Final Exam Date and Time for Fall 2014

<table>
<thead>
<tr>
<th>CLASSROOM</th>
<th>DATE</th>
<th>EXAM TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMCS-329</td>
<td>TUESDAY, DEC 16TH</td>
<td>4:00PM – 6:00PM</td>
</tr>
</tbody>
</table>
19. Acknowledgement

Please print your name, date, red-id, and signature to acknowledge that you understand the student expectations contained within, academic dishonesty policy, and have received the course syllabus.

________________________       ____________
Name            Red-ID

________________________  ____________
Signature        Date

* Please sign and return to your instructor, on the first or second day of class