Critical Infrastructure Protection (HMSY 1341) Online

Credit: 3 semester credit hours (3 hours lecture, 0 hours lab)

Prerequisite/Co-requisite: Complete the Online Orientation and answer yes to 7+ questions on the Online Learner Self-Assessment: http://www.lit.edu/depts/DistanceEd/OnlineOrientation/OOStep2.aspx

Course Description

Identification and analysis of critical infrastructure systems including security and threat assessments. Includes mitigation of threats as well as evaluation and revision of security measures in order to protect critical infrastructures. *This course is time-bound, structured, and completed totally online.*

Required Text and Materials

Text Material is provided online:

- A Guide to Critical Infrastructure Security and Resilience (November 2019)
- Critical Infrastructure Sectors_ CISA
- The Office of Infrastructure Protection
- IS-913.a Critical Infrastructure and Key Resources Support Annex
- IS-860.c National Infrastructure Protection Plan (NIPP), An Introduction
- IS-1170, Introduction to the Interagency Security Committee (ISC)
- IS-906 Workplace Security Awareness
- IS-907 Active Shooter: What You Can Do
- IS-914 Surveillance Awareness: What You Can Do
- IS-915 Protecting Critical Infrastructure Against Insider Threats

Course Objectives

Upon completion of this course, the student will be able to:

1. Identify local area critical infrastructures
2. Evaluate security measures
3. Report methods to revise security of protection assets
4. Demonstrate mitigation of a critical infrastructure threat
5. Conduct information collection using the Internet and library resources
6. Present written and oral reports on findings

Approved: 12/22

Course Outline

A. Syllabus Introduction
   1. Introduction of Faculty and students
   2. Instructor Bio
   3. Course Introduction and Overview

B. IS-860.c National Infrastructure Protection Plan (NIPP), An Introduction
   1. Describe NIPP 2013 key concepts across the entire critical infrastructure community - including private sector and government at all levels.
   2. Describe the core tenets and the values and assumptions considered when planning for critical infrastructure security and resilience.
   3. Identify activities critical partners may implement to achieve national goals aimed at enhancing critical infrastructure security and resilience put forward in the NIPP 2013 Call to Action.
   4. Describe ways to apply these concepts to support security and resilience within your community or area of responsibility.

C. IS-913.a Critical Infrastructure Security and Resilience: Achieving results through Partnership and Collaboration
   1. Explain the value of partnerships to infrastructure security and resilience.
   2. Identify strategies to build successful critical infrastructure partnerships.
   3. Describe methods to work effectively in a critical infrastructure partnership.
   4. Identify processes and techniques used to sustain critical infrastructure partnerships.
   5. Identify strategies and methods for achieving results through critical infrastructure partnerships.

D. The National Risk and Capability Assessment
   1. What threats and hazards can affect our community?
   2. If they occurred, what impacts would those threats and hazards have on our community?
   3. Based on those impacts, what capabilities should our community have?
   4. The outputs form this process lay the foundation for determining a community's capability gaps as part of the Stakeholder Preparedness Review.

E. IS-906: Workplace Security Awareness
   1. Identify potential risks to workplace security.
   2. Describe measures for improving workplace security.
   3. Determine the actions to take in response to a security situation

F. IS 907Active Shooter: What You Can Do
   1. Describe actions to take when confronted with an active shooter and responding law enforcement officials.
   2. Recognize potential workplace violence indicators.
   3. Describe actions to take to prevent and prepare for potential active shooter incidents.
   4. Describe how to manage the consequences of an active shooter incident.

G. IS-1170, Introduction to the Interagency Security Committee (ISC)
   1. Describe the history, vision, and mission of the ISC
   2. Describe how the ISC is organized
   3. Identify the Risk Management Process Standard

H. Critical Infrastructure Sectors_ CISA

1. Chemical Sector
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, materials, and Waste
15. Transportation Systems
16. Water and Wastewater Systems

I. A Guide to Critical Infrastructure Security and Resilience (November 2019)

1. What is Critical Infrastructure
2. What are the "Threats and Hazards" to Critical Infrastructure
3. Who is Responsible for Critical Infrastructure
4. What Drives Critical Infrastructure Security and Resilience
5. Getting Started
6. The Risk Management Framework
7. The Role of Risk Assessments
8. Training and Education
9. Evaluating the Program
10. Promoting the Program

J. IS-915 Protecting Critical Infrastructure Against Insider Threats

1. Describe the threat that malicious insiders pose to critical infrastructure.
2. Identify common characteristics and indicators associated with malicious insiders.
3. Identify actions that can be taken against insider threats.

K. IS-914 Surveillance Awareness: What You Can Do

1. Identify potential targets of adversarial surveillance.
2. Describe the information obtained by surveillance that is of interest to adversaries.
3. Recognize indicators of surveillance within the everyday environment.
4. Identify actions that you can take to detect potential adversarial surveillance incidents.
5. Describe the importance of identifying and reporting suspicious activities associated with adversarial surveillance.
6. Specify actions you can take to report potential incidents of adversarial surveillance.

L. 2019 National Threat & Hazard Identification and Risk Assessment (THIRA)

1. National THIRA Overview
2. Identify Methodology and Outputs
3. Describe Limitations and Future Research
4. Scenario Context Descriptions
5. Standardized Impacts
6. Scenario Chronology
7. Standardized Targets

M. About BRIC_ Reducing Risk through Hazard Mitigation

1. Discuss funding opportunities to build resilient infrastructure
2. Provide proactive methods for risk reduction

N. USFA Critical Infrastructure Protection Process Job Aid

1. Assist with the process of critical infrastructure protection.
2. Provide a template for the systematic protection of critical infrastructures.
3. Describe planning aspects easily adapted to assist infrastructure protection objectives of any community, service, department, agency or organization.

Grade Scale

90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
0 – 59	F

Course Evaluation

Final grades will be calculated according to the following criteria:

1. Tests	40%
2. Assignments	40%
3. Final Project	20%

Course Requirements

1. This course is time-bound, structured and completed totally online
2. During Week 1: there will be activities to familiarize the learner with the learning environment
3. You must log onto Blackboard 2-3 times each week.
4. Complete the assignments and tests.
5. You must participate in online discussions each week.
6. Prerequisite - Completed the Online Orientation and answered 5+ questions correctly on the Online Learner Self-Assessment: http://www.lit.edu/depts/DistanceEd/OnlineOrientation/OOStep2.aspx
7. Tests are graded automatically upon completion.
8. Students research a critical infrastructure sector and compose a four-page report. The report will be double spaced and written in Arial 12 font. Footnotes and references are required.
9. Students may call during office hours and can also arrange call times through email.
10. The Instructor will respond to e-mail communication within 24-72 hours.

Course Policies

1. Tests will be automatically grade and recorded in Blackboard.
2. Cheating of any kind will not be tolerated.
3. Students are expected to use proper net etiquette while participating in course emails, assignment submissions, and online discussions.
4. Your final grade will be the average of your weekly assignments, tests, discussions, and the Final Project.
5. If you wish to drop a course, the student is responsible for initiating and completing the drop process.
6. If you do not complete assignments and tests or fail to drop the course, you will earn an ‘F’ in the course.

Technical Requirements

The latest technical requirements, including hardware, compatible browsers, operating systems, software, Java, etc. can be found online at: http://kb.blackboard.com/pages/viewpage.action?pageId=71860304

A functional broadband internet connection, such as DSL, cable, or WiFi is necessary to maximize the use of the online technology and resources.

Disabilities Statement

The Americans with Disabilities Act of 1992 and Section 504 of the Rehabilitation Act of 1973 are federal anti-discrimination statutes that provide comprehensive civil rights for persons with disabilities. Among other things, these statutes require that all students with documented disabilities be guaranteed a learning environment that provides for reasonable accommodations for their disabilities. If you believe you have a disability requiring an accommodation, please contact the Special Populations Coordinator at (409) 880-1737 or visit the online resource: http://www.lit.edu/depts/stuserv/special/defaults.aspx

Student Code of Conduct Statement

It is the responsibility of all registered Lamar Institute of Technology students to access, read, understand and abide by all published policies, regulations, and procedures listed in the *LIT Catalog and Student Handbook*. The *LIT Catalog and Student Handbook* may be accessed at www.lit.edu or obtained in print upon request at the Student Services Office. Please note that the online version of the *LIT Catalog and Student Handbook* supersedes all other versions of the same document.

Starfish

LIT utilizes an early alert system called Starfish. Throughout the semester, you may receive emails from Starfish regarding your course grades, attendance, or academic performance. Faculty members record student attendance, raise flags and kudos to express concern or give praise, and you can make an appointment with faculty and staff all through the Starfish home page. You can also login to Blackboard or MyLIT and click on the Starfish link to view academic alerts and detailed information. It is the responsibility of the student to pay attention to these emails and information in Starfish and consider taking the recommended actions. Starfish is used to help you be a successful student at LIT.