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:
1. Critical Infrastructure Resource Guide 2010
2. IS-821 Critical Infrastructure and Key Resources Support Annex
3. IS-860.a National Infrastructure Protection Plan (NIPP)
4. IS-890.a, Introduction to the Interagency Security Committee (ISC)
5. IS-906 Workplace Security Awareness
6. IS 907 Active Shooter: What You Can Do
7. IS-912 Retail Security Awareness: Understanding the Hidden Hazards
8. IS-921 Implementing Critical Infrastructure Protection Programs

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.

Course Outline

1. Syllabus
   a. Introduction of Faculty and students
   b. Instructor Resume
   c. Comments
2. IS-860.a National Infrastructure Protection Plan (NIPP)
   a. Protecting and ensuring the resiliency of the critical infrastructure and key resources of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life.
   b. The purpose of this course is to present an overview of the National Infrastructure Protection Plan (NIPP).
   c. The NIPP provides the unifying structure for the integration of existing and future CIKR protection and resiliency efforts into a single national program.

Approved 11/2020

3. IS-821 Critical Infrastructure and Key Resources Support Annex
   a. The National Response Framework (NRF) presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies.
   b. The NRF, Support Annexes describe how Federal departments and agencies, the private sector, volunteer organizations, and nongovernmental organizations (NGOs) coordinate and execute the common support processes and administrative tasks required during an incident.
   c. The actions described in the Support Annexes are not limited to particular types of events, but are overarching in nature and applicable to nearly every type of incident.
   d. This course provides an introduction to the Critical Infrastructure and Key Resources (CIKR) Support Annex to the NRF.
4. The Office of Infrastructure Protection
   a. State what the specific risks are in their locations and to their industries;
   b. Discuss how to coordinate with others within and across sectors and share vital information
   c. Explain how to prepare, protect, and respond
   d. List the six programmatic areas of IP.
5. IS-913.a Critical Infrastructure Security and Resilience: Achieving Results through Partnerships and Collaborations;
   a. The purpose of this course is to introduce the skills and tools to effectively achieve results for critical infrastructure security and resilience through partnership and collaboration.
   b. Explain the value of partnerships to infrastructure security and resilience.
   c. Identify strategies to build successful critical infrastructure partnerships.
   d. Describe methods to work effectively in a critical infrastructure partnership.
   e. Identify processes and techniques used to sustain critical infrastructure partnerships.
   f. Identify strategies and methods for achieving results through critical infrastructure partnerships.
6. IS-921.A: Implementing Critical Infrastructure Security and Resilience
   a. This course introduces those with critical infrastructure duties and responsibilities at the State, local, tribal, and territorial levels to the information they need and the resources available to them in the execution of the mission to secure and improve resilience in the Nation's critical infrastructure.
   b. Summarize critical infrastructure responsibilities.
   c. Identify the range of critical infrastructure government and private-

sector partners at the State, local, tribal, territorial, regional, and Federal levels.
   d. Describe processes for effective information sharing with critical infrastructure partners.
   e. Identify various methods for assessing and validating information.
7. IS-912: Retail Security Awareness: Understanding the Hidden Hazards
   a. The purpose of this course is to make persons involved in commercial retail operations aware of the actions they can take to identify and report suspicious purchases or thefts of products that actors could use in terrorist or other criminal activities.
   b. To achieve this goal, the course provides an overview of prevention steps aimed at identifying and monitoring high-risk inventory products and reporting suspicious activities to law enforcement agencies.
   c. Identify steps they can take to help prevent their inventory from being used to manufacture or deploy homemade explosives.
   d. Describe the importance of identifying and reporting suspicious purchases and activities in the retail sector.
   e. Specify additional actions they can take to protect their inventory from misuse or theft.
8. IS-906: Workplace Security Awareness

   a. This course provides guidance to individuals and organizations on how to improve the security in your workplace.
   b. We live in a world of ever-increasing risk.
   c. No workplace – be it a construction site, office building, factory floor, or retail store – is immune from these threats.
   d. Risks threaten worker safety, employee morale, and your company's economic livelihood.
9. IS 907: Active Shooter: What You Can Do
   a. An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and other populated area.
   b. In most cases, active shooters use firearms and there is no pattern or method to their selection of victims.
   c. Active shooter situations are unpredictable and evolve quickly.
   d. All employees can help prevent and prepare for potential active shooter situations.
10. IS-909: Community Preparedness: Implementing Simple Activities for Everyone
    a. Community members are the key to our Nation's preparedness and resilience. As such, we need to:
    b. Support the development of prepared, vigilant, and engaged communities.
    c. Foster strategic partnerships among:
    d. The private sector.

e. Nongovernmental organizations.
f. Foundations.
g. Community-based organizations.
h. Identify the definition of preparedness.
i. Describe the role of individuals and households in preparedness.
j. Identify community preparedness principles.
k. Describe the purpose of community-based preparedness activities.
l. Identify the steps for planning and conducting a community-based preparedness program.
m. Identify resources for supporting community-based preparedness programs.

11. IS-914: Surveillance Awareness: What You Can Do
a. The purpose of this course is to make critical infrastructure employees and service providers aware of actions they can take to detect and report suspicious activities associated with adversarial surveillance.
b. To achieve this goal, the course provides an overview of surveillance activities and the indicators associated with them, as well as the actions that employees and service providers can take to report potential surveillance incidents.
c. Identify potential targets of adversarial surveillance.
d. Describe the information obtained by surveillance that is of interest to adversaries.
e. Recognize indicators of surveillance within the everyday environment.
f. Identify actions that you can take to detect potential adversarial surveillance incidents.
g. Describe the importance of identifying and reporting suspicious activities associated with adversarial surveillance.
h. Specify actions you can take to report potential incidents of adversarial surveillance.

12. IS-915: Protecting Critical Infrastructure Against Insider Threats
a. This course provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure.
b. Describe the threat that malicious insiders pose to critical infrastructure.
c. Identify common characteristics and indicators associated with malicious insiders.
d. Identify actions that can be taken against insider threats.

13. IS-916: Critical Infrastructure Security: Theft and Diversion – What You Can Do
a. This course introduces

critical infrastructure personnel to the information they need and the resources available to them to identify threats and vulnerabilities to critical infrastructure from the theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. The course also identifies actions that participants can take to reduce or prevent theft and diversion.

b. Describe the threat that theft and diversion pose to critical infrastructure protection and resilience.

c. Recognize which of your resources, raw materials, products, or technologies are vulnerable to theft and

15. Critical Infrastructure Resource Guide

  a. The Critical Infrastructure Working Groups

    i. Agriculture and Food
    ii. Banking and Finance
    iii. Chemical Sector
    iv. Commercial Facilities
    v. Communications
    vi. Critical Manufacturing
    vii. Dams
    viii. Defense Industry Base

diversion.

d. Identify commonly used theft and diversion methods and schemes.

e. Recognize suspicious behaviors and activities associated with theft and diversion.

f. Identify measures for protecting against theft and diversion.

14. Introduction to the Interagency Security Committee (ISC) is the first course in the ISC Web-based training series.

  a. The purpose of this series of courses is to provide Federal facility security professionals, engineers, building owners, construction contractors, architects, and the general public with basic information pertaining to the ISC and its facility security standards, processes, and practices.

    ix. Emergency Services
    x. Energy
    xi. Government Facilities
    xii. Healthcare and Public Health
    xiii. Information Technology
    xiv. National Monuments and Icons
    xv. Nuclear Reactors, Materials, and Waste
    xvi. Postal and Shipping
    xvii. Transportation Systems
    xviii. Water

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   5%
2. Assignments   40%
3. Module Discussions   15%
4. Final Project   40%

Course Policies

1. You must log onto Blackboard and access this course a minimum of three times per week.
2. Cheating of any kind will <u>not</u> be tolerated.
3. If you wish to drop a course, the student is responsible for initiating and dropping the course. If you stop logging-in to the course and do not complete the course drop process, then you will receive an "F" grade for the course
4. Internet Usage – Students are expected to use proper net etiquette while participating in course emails, assignment submissions, and online discussions.

Technical Requirements (for courses using Blackboard)

The latest technical requirements, including hardware, compatible browsers, operating systems, software, Java, etc. can be found online at:
https://help.blackboard.com/en-us/Learn/9.1_2014_04/Student/015_Browser_Support/015_Browser_Support_Policy 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.

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.