STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

COURSE OUTLINE

JUST 420 – THE CORPORATE ROLE IN HOMELAND SECURITY

Prepared By: Paul R. Bowdre

SCHOOL OF SCIENCE, HEALTH AND CRIMINAL JUSTICE
CRIMINAL JUSTICE DEPARTMENT
MAY 2015

A. **TITLE**: The Corporate Role in Homeland Security

B. **COURSE NUMBER:** JUST 420

C. **CREDIT HOURS:** 3

D. **WRITING INTENSIVE COURSE**: No

E. **COURSE LENGTH:** 15 weeks

F. **SEMESTER(S) OFFERED:** Fall

G. **HOURS OF LECTURE, LABORATORY, RECITATION, TUTORIAL, ACTIVITY:** 3 lecture hours per week

H. **CATALOG DESCRIPTION:** This course explores the role of private sector entities in Homeland Security and relationships with governmental Homeland security agencies. It examines the specific roles, responsibilities, and vulnerabilities of corporate entities in protecting the infrastructure as well as preventing, deterring, and responding to events. Institutions such as utility providers, the private security industry, mental health systems, hospitals and biomedical facilities, companies with chemical and hazardous materials inventories, shipping and transportation companies, airlines and airports, the financial services industry, and information technology and telecommunications companys are considered.

I. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): Fundamentals of Homeland Security (JUST 230) and completion of 45 semester credits in Criminal Investigation, Criminal Justice: Law Enforcement Leadership or Homeland Security or permission of the instructor
b. Co-requisite(s): None

J. **GOALS (STUDENT LEARNING OUTCOMES):** By the end of this course, the student will be able to:

.

Course Objective	*Institutional SLO*
1. Identify the direct impact of modern day terrorism on corporate operations.	3. Professional Competence
2. Summarize private sector roles, responsibilities, and relationships with public sector entities involved with Homeland Security.	1. Communication 3. Professional Competence
3. Articulate the vulnerabilities of corporate entities in critical incidents.	1. Communication 3. Professional Competence
4. Explain the role of private sector entities in protecting the infrastructure.	1. Communication 3. Professional Competence

5. Illustrate the best methods of preventing, deterring, and responding to critical incidents.	1. Communication 3. Professional Competence
6. Explain the process of development of readiness plans for private sector institutions.	1. Communication 3. Professional Competence

K. TEXT:

Lee, E. (2015). Homeland security and private sector business: Corporations' role in critical infrastructure protection (2nd ed.). Boca Raton, FL: CRC Press.

L. REFERENCES:

Kamien, D.G. (Ed.) (2012). *Homeland security handbook* (2nd ed.). New York, NY: McGraw-Hill.

Kraft, M.B. & Marks, E. (2012). *U.S. government counterterrorism: A guide to who does what.* Boca Raton, FL: Taylor & Francis Group.

"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." PL 107-56.

M. EQUIPMENT:

- Technology enhanced classroom
- Simulated firearms and edged weapons
- Training handcuffs

N. GRADING METHOD: A-F

O. MEASUREMENT CRITERIA/METHODS:

- Exams
- Quizzes
- Papers
- Participation

P. DETAILED COURSE OUTLINE:

I. Introduction: Homeland Security Vision
   A. The desired state of homeland security
   B. The current state of homeland security
   C. Homeland security issues and challenges
   D. Everyone has a role in homeland security

E. History of terrorism
F. The direct impact of modern-day terrorism
G. What is at stake with today's terrorist attacks
H. Countering terrorism with help from the Department of Homeland Security
I. Help from the Department of Homeland Security is not enough

II. Essential Threat Factors
A. The problem we face with threats
B. General threats to security hierarchy components
C. General threats effect on homeland security
D. Threat management through intelligence
E. Terrorists' operational methodology
F. Limitation of early warnings
G. Post-9/11 era threats and warnings
H. Creating your own threat-warning capabilities
I. Painful lesson: The USS Cole attack
J. The consequences of not understanding threats
K. Lessons learned: First World Trade Center attack, 1993
L. Lessons learned: First American hijacking, 1961
M. Homeland security roles and misconceptions

III. National Infrastructure Protection Plan for Threats, Vulnerability, Risk, and Resilience
A. The DHS risk model and NIPP
B. Infrastructure protection plan (NIPP)
C. Responsibility and accountability per DHS
D. NIPP as a template
E. A practical framework for taking the NIPP approach
F. A practical framework for assessing threat
G. How to handle discoveries of threat and vulnerabilities
H. Determining vulnerability
I. Simplified assessment model
J. Countermeasures
K. Methods for small business security practices

IV. Risk Mitigation, Transference, and Elimination
A. Risk decision principles
B. Risk management
C. Lessons not easily learned

V. Readiness Plans: Develop, Validate, and Update
A. How terrorists plan
B. Collaboration with external organizations
C. Preplan development process
D. Plan deployment
E. Overlooked plan items

F. Plan validation and maintenance
G. Plan updates
H. Plan to share information
I. What the DHS says about protected critical infrastructure information

VI. Prevention, Detection, and Response Factors across Sectors
A. Innovative prevention approaches
B. Innovative detection technology
C. Investing in response capabilities through partnership
D. Response considerations
E. Preparation snapshot
F. Historical case study

VII. Human Factors and Team Dynamics
A. The human factor
B. Humanity in crisis and hero mode
C. Female terrorists: The human factor gone wrong
D. Humans in conflict
E. Overconfidence
F. Human technology
G. Superdiversity
H. Diversity as a problem solver
I. The human factor as a tool
J. Dysfunctional group dynamics
K. Discussion versus dialogue
L. How to get your team to dialogue
M. Leadership versus management

VIII. Innovative Ideas for Change
A. Organizational leadership
B. Why workforce breakdown is critical
C. Group roles and team roles
D. Low-context and high-context communications
E. Reactive versus proactive language
F. The forming, storming, norming, performance model

IX. Training and Exercises: Touch It, Feel It, Live It, Breathe It
A. Benefits of training
B. Adult learning
C. Training methods
D. Crawl-Walk-Run methodology
E. Training evaluation
F. Educational programs
G. Training failures
H. A subjective method for calculating return on investment (ROI)

X. You Can Deter, But You Can't Interdict: Don't Cross the Line!
   A. Know thy limits
   B. Distinctions between collecting information and collecting intelligence
   C. How to avoid botching an investigation
   D. Stumbling across evidence of a crime: How to preserve it and relinquish it to law enforcement agencies

Q. <u>LABORATORY OUTLINE</u>: N/A