DSS CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)
EDUCATION DIVISION

Managing a DoD Installation Security Program
ED 507

SAMPLE COURSE SYLLABUS*

A. DESCRIPTION

The *2007 Defense Installations Plan* created a strategic vision for the management of facilities within the DoD. The forward to this document is instructive to those seeking to understand the role of installations within the Department:

> "America's security depends upon defense installation assets that are available when and where needed, and with the right capabilities to support current and future mission requirements. As the enterprise managers of the defense installations portfolio, we recognize transformation as a critical enabler to ensure these capabilities are delivered —– effectively and efficiently.
>
> America's military installations, including their associated environment, have many purposes. They must sustain the regular forward and home station presence of U.S. forces as well as provide support in training and deployment to meet the Nation's need in periods of crisis, contingency, and combat. They need to ensure a productive, safe, and efficient workplace, and also offer a decent quality of life for military members and families, and the civilian and contactor workforce.
>
> The President and the Secretary of Defense have challenged the military to transform itself to meet current and future threats to America's security. In addition to leading-edge weapon systems, doctrinal innovation, and the employment of technology, this transformation also requires a similar change in our approach to the fundamental business practices and infrastructure "backbone" of the Department of Defense."

Goal 3 of this Plan is entitled "Right Risk" and articulates the Department's concept for the protection of its installations:

"DoD leaders must be able to anticipate, recognize, evaluate, and manage risk while maintaining the capability to respond and recover from incidents that degrade the mission……. DoD is dedicated to identifying and mitigating or avoiding unnecessary and unacceptable risk."

Further guidance for the protection of DoD installations was provided in DoD Instruction 6055.17 titled *DoD Installation Emergency Management (IEM) Program*, dated January 13,

*Sample syllabus is subject to change each semester.

2009. This Instruction aligns DoD emergency management (EM) activities with the National Incident Management System (NIMS), the National Preparedness Guidelines (NPG), and the National Response Framework (NRF). Among the directives in this Instruction are:

a. Maintain DoD readiness by establishing and maintaining a comprehensive, all-hazards IEM Program on DoD installations worldwide.
b. Support and assist U.S. civil authorities, as directed, in EM activities for mitigating, preventing, planning for, responding to, and recovering from a natural or manmade disaster or hazard.
c. Adopt and implement procedures consistent with NIMS and the incident command system (ICS) in accordance with the Deputy Secretary of Defense Memorandum *Homeland Security Presidential Directive 5*.
d. Adopt and implement, as appropriate, IEM program management, emergency planning, and continuity planning.
e. Support the implementation of the NRF within the United States through the development, implementation, and sustainment of the DoD IEM Program detailed in this Instruction.
f. Coordinate preparedness, response, and recovery requirements and capabilities with State, local, and tribal governments; other Military Department(s); or host-nation partners using an all-hazards approach that balances risk management (i.e., threat, vulnerability, and consequence), resources, and need.

Because security is diffused among a variety of separate functional areas within the DoD, and the military services and DoD agencies have their own policies concerning installation security, the responsibility for coordinating and managing the execution of the installation program falls on the security professional. Critical to the development of a security leader and manager is a comprehensive and practical knowledge of DoD security programs and the ability to synchronize their execution within the broad parameters and limited resources of a DoD installation management organization. Accordingly, CDSE has established as a primary goal the development of future security leaders who are adept generalists across the wide range of DoD security responsibilities rather than being focused specialists. To accomplish this goal, CDSE has created a graduate program in Defense Security Studies, with the *Managing a DoD Installation Security Program* course as an important part of the overall program.

At <u>no</u> time in the course shall any participant introduce by any means classified information. This course is <u>only</u> comprised of unclassified information. If in doubt on any information, do not use it in this class and consult with your unit or installation security manager. For Official Use Only (FOUO) information may be discussed in this class within the Sakai environment. Whenever FOUO information is introduced into the class it should be identified as FOUO and protected in accordance with all applicable regulations.

The *Managing a DoD Installation Security Program* course covers the ways in which the senior security manager can apply a knowledge of DoD security requirements to lead development of a comprehensive, capabilities-based installation security plan through the use of appropriate risk management techniques. Once a plan is developed, the security professional must be able to evaluate its effectiveness and recommend changes where necessary. The first half of the course establishes the context and basics of DoD security management at the installation level, and the second half of the course builds on that knowledge through application in a variety of common security management scenarios. Specifically, the course will address:

1. The various requirements for an installation security program
2. How to manage an installation security program, including managing the security office budget and manpower
3. The importance of security manager interaction with the intelligence and counterintelligence community
4. Organizing installation assets to support the security plan
5. Training security personnel and promoting public awareness
6. Determining installation security equipment requirements
7. Planning for and managing the costs of security systems acquisitions
8. Designing, developing, conducting, and evaluating an installation training and exercise program
9. Developing and managing a corrective action program to address known deficiencies
10. Liaison with local authorities
11. Case studies/practical exercises

This is not a "skills" training course designed to produce expert security managers or even managers knowledgeable of the intricacies of each Service's and Agency's security systems and practices. Instead, this course is designed to provide the student with a thorough grasp of the principles and techniques for sound security planning, program justification, and budget management within the DoD installation environment so that he or she can quickly adapt to the unique specifics of each organization and perform security program management effectively.

Because this class is designed for security professionals with varying levels of expertise in differing security disciplines, it is anticipated that the combined efforts of all class participants will stimulate discussion and the exchange of ideas while driving the learning environment. Accordingly, adequate class preparation will be required to successfully complete this course.

B. ORGANIZATION

This is a graduate-level distance-learning course in DoD installation security management. The course will consist of textbook and other, readings, lectures and presentations, participation in discussion forums, a case study, and two practical exercises.

Because this is a 3 credit hour equivalent course, the contact time over the 16 weeks should be approximately 40 hours.

Students will be required to critically analyze and discuss the readings as well as to be able to articulate them from differing perspectives.

Students will be expected to do research at the graduate level in this course. To provide a substantial research capability to all students in the program, a number of internet-accessible research sites will be sent to each student prior to the first lesson. The primary research site will be the CiteULike virtual library. Students will also receive information for signing on to other research sites or databases relevant to security and defense studies, such as opening an account with the Defense Technical Information Center (DTIC). This will ensure that every student has more than enough resources to do the research expected in this course. The instructor may provide additional research sources or sites. Students are also encouraged to make use of library and research sources available to them in their own geographical area or through their own professional or academic networks. Wikipedia cannot not be used as a reference.

Class participation is both important and required. If, due to an emergency, students are unable to respond to a discussion prompt in the week it is assigned, they must contact the instructor immediately.

The academic week begins at 0001 Eastern Time (ET) on the Monday of that week. It ends at 2359 ET on the Sunday of that week. No discussion posts nor specific graded assignments can be submitted before the week they are due.

Discussion Forum:

A. Students must post responses to all instructor provided discussion questions, two per week, no later than Wednesday, 2100 ET each week. Each posting must be at least 250 words in length and have a minimum of two references (books, articles, etc.) in accordance with the *Chicago Manual of Style*, 16th Ed.
B. To facilitate learning and discussion, students will also respond to at least two other students responses no later than Friday, 2359 ET each week. Any research references used must be annotated in accordance with the *Chicago Manual of Style*, 16th Ed. Points will be lost for non-participation or not providing thoughtful comments on at least two others students post.
C. Posting and responding is encouraged as early in the week as possible. This gives other students more time to read and respond to more students' posts, thus enhancing learning. It is important that a group discussion be built by asking each other questions, thoughtfully responding to other students' posts, expanding on points from different perspectives, offering a resource or a tip, giving personal examples, or playing "devil's

advocate".

Specific Graded Assignments: There are three: one case study and two practical exercises. These must be posted by 2359 ET on Sunday during the week they are due. For example, if the syllabus states the graded assignment is due in week 4, the assignment must be submitted no later than 2359 ET on Sunday, the last day of week 4. These assignments must have at least four references to support the assignment annotated in accordance with the *Chicago Manual of Style*, 16th Ed. Every effort should be made to submit the assignments on time.

It is expected that assignments will be submitted on time; however, it is recognized that students occasionally have serious work/personal problems that prevent work completion by the deadline. If such a dilemma arises, students should contact the instructor immediately.

C. OBJECTIVES

This course will enable students to:

- Examine the mission of a typical DoD installation
- Describe the organization of a typical DoD installation
- Explain the mission of the installation security manager and the typical organization of an installation security office, to include the management of security office resources
- Articulate the relationship among the security manager, installation staff, and the installation commander/manager, including the interface with intelligence agencies
- Assess the risk to a DoD installation
- Assess the unique security requirements of a DoD installation
- Apply the principles of sound risk management to the evaluation of an existing security program
- Evaluate the likelihood of a security program achieving its protection mission
- Analyze the effectiveness of an organization dedicated to a security program
- Analyze the training program related to a security program
- Evaluate the appropriateness of equipment associated with a security program
- Evaluate a security program exercise plan
- Evaluate the ability of a security program to achieve its protection mission
- Assess the effectiveness of a corrective action program
- Evaluate the level of cooperation with local security officials

D. COURSE REQUIREMENTS

Evaluation criteria for each graded assignment aside from discussion questions are listed below. Any assignment that receives a failing grade can be resubmitted within the following two weeks, but there will be no further extensions beyond this two-week period. If a student receives a failing grade on assignment, contact the instructor.

Expectation for Participation (20%): Participation includes preparing for class, participating in online class activities, participating in class exercises, and reflecting on the experience after class by way of a private journal to be submitted at the end of the semester. To achieve full credit for participation, learners must attend, participate, and reflect. Learners are expected to attend all classes; however, learners are permitted to miss two class sessions without it adversely affecting their final course grade. Class attendance in the context of this course is defined as participation in scheduled online activities.

Practical Exercise I Execution (25%): This project will require the students to perform a risk assessment and determine the capabilities necessary to adequately protect an installation from an all-hazards threat. It will also address the capabilities required by an installation to properly respond to, and recover from, a specified threat. Students will be required to analyze a situation and use the Target Capabilities List to determine if the installation is prepared. Student responses will require application of principles learned in Lessons 2 – 10. Detailed instructions will be provided in a handout.

Practical Exercise II Execution (25%): This project will require the students to develop an exercise program for a DoD installation focused on assessing the capabilities necessary to adequately protect the installation from an all-hazards threat. It will also assess the capability of the installation to properly respond to, and recover from, a specified threat. Students will be required to design, develop, conduct, and evaluate an exercise. Student responses will require application of principles learned in Lessons 12 – 13. Detailed instructions will be provided in a handout.

Case Study and Presentation (30%): Each student will be required to choose a topic about which they will perform research, write a case study, and prepare a presentation for the class. A list of topics from which students might choose will be available, but students are also free to suggest a topic to the instructor for approval. Students are encouraged to select topics that relate to their current position or future career goals. Such a project would be designed to enhance the student's value in the workplace and/or prepare the student to assume different or greater responsibility within the DoD. At the end of the semester, each student will post a PowerPoint presentation summarizing the salient findings of his/her case study along with at least three discussion topics, about which other students will offer online comments. Research papers will be formatted using *The Chicago Manual of Style, 16th Edition*, Chicago: University of Chicago Press, 2010.

E. GRADING

The following provides a breakdown of how each assignment contributes to the overall grading criteria. The following provides an approximate breakdown of how each assignment

contributes to the overall performance in the class.

Category	Weight	Point Value
Class Participation	20%	200
Practical Exercise I Execution	25%	250
Practical Exercise II Execution	35%	250
Case Study and Presentation	30%	300
Total	**100%**	**1,000**

Individual graded assignments with a score lower than 80% are acceptable; however, a student's final grade at the end of the semester must be 80% or higher to pass the course.

A letter grade will be assigned to each graded assignment, following the grading scale below:

Letter Grade	Point Range	Percentage
A	900 -1000	90-100%
B	800-899	80-89%
C	700-799	70-79%
D	600-699	60-69%
F	599 and below	59% and below

Evaluation criteria for each graded assignment are listed below.

Element Evaluated	Evaluation Criteria			
	Excellent 90-100%	**Good 80-89%**	**Below Standards 70-79%**	**Failure 69 or below%**
Content of paper, analysis, presentation, or project (40% of paper's grade)	Critical thinking related to the issues, substance, points raised and arguments presented is very evident	Critical thinking is well demonstrated	Some critical thinking is shown but could improve	Critical thinking is not well demonstrated or not evident
Application of theory and knowledge to given facts (30%)	Application of theory and knowledge is very evident	A good understanding of theory and knowledge is shown	Some understanding of theory and knowledge is shown	Understanding of theory and knowledge is lacking in significant respects or absent
Completeness (15%)	Assignment is complete in every aspect and exceeds requirements	Assignment is complete	Assignment is mostly complete but missing some required elements	Assignment is missing major elements
Terminology (5%)	Use of terminology is correct in all instances	Terminology is mostly correct	Multiple mistakes in terminology	Correct terminology not used
Organization / Style (5%) Form (grammar, format, punctuation, spelling, logic) citation)	Organization is relevant to topic, clear and understandable with logical flow Virtually error free.	Mostly relevant, clear, and logical Few errors (one per page or less)	Unclear, Lacks relevance, is difficult to understand, or logic is missing. Frequent Errors (over one per page)	Disorganized, improper style. Form errors endemic throughout.

F. COURSE TEXTBOOKS /READINGS

There is no single textbook available that can address all of the instructional needs for this class. However, *Strategic Security Management: A Risk Assessment Guide for Decision Makers* by Karim H. Vellani is an excellent resource for DoD security professionals who make risk management recommendations and decisions daily. It is the only required textbook for the class. Many of the course readings will be from this textbook. Additionally, the instructor will assign periodically readings collected from print and online resources. Students are encouraged to establish personal professional libraries to enhance their learning and serve as references for future security endeavors.

Required Text:

Vellani, Karim H. *Strategic Security Management: A Risk Assessment Guide for Decision Makers*, Burlington, MA: Butterworth-Heinemann/Elsevier, Inc., 2007.

Recommended But Not Required Text:

The Chicago Manual of Style, 16th Edition, Chicago: University of Chicago Press, 2010.

G. COURSE OUTLINE

The following table outlines the 16-week course agenda.

Week	Topics	Instructional Method	Student Assignments Due
1	• Course Overview, Grading, and Major Assignments • Introductions: Instructor and Students • Principles of Installation Security Management • Discuss Case Study Assignment	• Reading • Discussion forum • Asynchronous presentation	• Post biographical sketch prior to class • Introductions
2	• The DoD Installation Security Environment ▪ Programs ▪ Manpower ▪ Budgeting	• Reading • Discussion • Asynchronous presentation	• Discussion Forum (DF) 1: Respond to instructor discussion questions and other student responses

Week	Topics	Instructional Method	Student Assignments Due
3	• Principles of Risk Management ▪ Key Components ▪ Threat and Vulnerability Assessments	• Reading • Discussion • Asynchronous presentation	• DF 2: Respond to instructor discussion questions and other student responses
4	• The Federal Emergency Management System ▪ National Incident Management System (NIMS)National Preparedness Guidelines (NPG) National Response Framework (NRF)	• Reading • Discussion • Asynchronous presentation	• DF 3: Respond to instructor discussion questions and other student responses
5	• Target Capabilities List ▪ Key Components ▪ Risk Factors ▪ Using the TCL ▪ Mission Areas	• Reading • Discussion • Asynchronous presentation	• DF 4: Respond to instructor discussion questions and other student responses
6	• Common Target Capabilities ▪ Planning ▪ Communications ▪ Community Preparedness and Participation ▪ Intelligence and Information Sharing and Dissemination	• Reading • Discussion • Asynchronous presentation	• DF 5: Respond to instructor discussion questions and other student responses
7	• Prevent Mission Area ▪ Information Gathering and Recognition of Indicators and Warnings ▪ Intelligence Analysis and Production ▪ Counter-Terror Investigation and Law Enforcement ▪ CBRNE Detection	• Reading • Discussion • Asynchronous presentation	• DF 6: Respond to instructor discussion questions and other student responses

Week	Topics	Instructional Method	Student Assignments Due
8	• Protect Mission Area ▪ Critical Infrastructure Protection ▪ Food Safety and Defense ▪ Epidemiological Surveillance and Investigation ▪ Laboratory Testing	• Reading • Discussion • Asynchronous presentation	• DF 7: Respond to instructor discussion questions and other student responses
9	• Response Mission Area ▪ On-Site Incident Management ▪ EOC Management ▪ Critical Resource Logistics and Distribution ▪ Emergency Public Safety and Security Response ▪ Explosive Device Response	• Reading • Discussion • Asynchronous presentation	• DF 8: Respond to instructor discussion questions and other student responses
10	• Recover Mission Area ▪ Structural Damage Assessment ▪ Restoration of Lifelines ▪ Economic and Community Recovery	• Reading • Discussion • Asynchronous presentation	• DF 9: Respond to instructor discussion questions and other student responses • Prepare for Practical Exercise I
11	• Practical Exercise: Determining Required Capabilities for a DoD Installation	• Powerpoint presentation to class • Discussion • Asynchronous presentation	• Read Practical Exercise I Handout • DF 10: Respond to scenario discussion questions and other student responses
12	• Homeland Security Exercise and Evaluation Program (HSEEP) • Volume I: Overview and Exercise Program Management • Volume II: Exercise Planning and Conduct	• Reading • Discussion • Asynchronous presentation	• DF 11: Respond to instructor discussion questions and other student responses

Week	Topics	Instructional Method	Student Assignments Due
13	• Homeland Security Exercise and Evaluation Program (HSEEP) ▪ Volume III: Exercise Evaluation and Improvement Planning ▪ Volume V: Prevention Exercises	• Reading • Discussion • Asynchronous presentation	• DF 12: Respond to instructor discussion questions and other student responses • Prepare for Practical Exercise II
14	• Practical Exercise II ▪ Developing an Installation Exercise ▪ Conducting an Installation Exercise	• Powerpoint presentation to class • Discussion • Asynchronous presentation	• Read Practical Exercise II Handout • DF 13: Respond to scenario discussion questions and other student responses
15	• Practical Exercise II (cont'd) ▪ Developing and Managing a Corrective Action Program	• Powerpoint presentation to class • Discussion • Asynchronous presentation	• Read Practical Exercise II Handout • DF 14: Respond to scenario discussion questions and other student responses
16	• Case Study Submission • Course Wrap-Up and Critique	• Powerpoint presentation to class • Discussion • Asynchronous presentation	• Complete and submit Case Studies • DF 15: Respond to case study discussion questions and other student responses