DSS CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)
EDUCATION DIVISION
Security as an Integral Part of DoD Programs

SAMPLE COURSE SYLLABUS*

A. DESCRIPTION

The SIPDDP course is a comprehensive study of defense security as a cross-disciplinary function that supports the missions of DoD commands and agencies. This course will:

1. Address DoD security as a profession, and review the broad scope of disciplines and responsibilities within the security field with an eye toward how these skills and disciplines integrate into a program
2. Provide a strategic perspective on the function of security across disciplines and DoD organizations, establishing a foundation for other courses in the CDSE graduate curriculum
3. Address the emerging role of the multidisciplinary security generalist in contrast to the more narrowly focused security specialist

This is not a “skills” training course. It is a survey of the landscape that makes up DoD security. Because of the amount of material to be covered, no one topic will be covered with enough depth to develop expertise in that topic. Rather, students who may have been exposed only to narrow aspects of security in the past will be introduced to the broader scope of responsibilities that make up the DoD security portfolio.

The course is divided into two distinct parts. The first seven weeks will cover the basic functions and disciplines of DoD security. The remaining weeks will cover other specialty functions in which security professionals find themselves engaged. Through the introduction of new ideas, students will begin to consider how these disparate disciplines integrate into the larger DoD security effort.

B. ORGANIZATION

The primary methods of instruction will be short lectures, readings, student preparation of 1–2 page papers on the readings, and discussions on the issues brought forth in the lectures, readings and papers. 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.

Course Objectives

1. Analyze, explain and assess the broad scope of disciplines and functions within the DoD security arena
2. Examine and analyze critical and emergent issues within the DoD security disciplines and functions
3. Assess and analyze the costs and effects of policy decisions on the security program and its interrelationships with other DoD programs

*Sample syllabus is subject to change each semester.

4. Identify, analyze and explain the strategic effects of security program success or failure within the DoD
5. Assess and summarize the broad scope of competencies of a security generalist

Delivery Method/Course Requirements:

This is a graduate-level distance-learning course in security as an integral part of DoD programs. The course will consist of readings, prerecorded lectures and presentations, participation in the discussion forum, written assignments, and midterm and final exams.

A typical week will include a 45-60 minute prerecorded lecture, with the remainder of the week being dedicated to readings relevant to the week's topic and a discussion of those readings in the course discussion forum. Students should be prepared to critically discuss and debate the readings as well as analyze them for biases and multiple perspectives. Though the course covers only one topic per week, students should also be examining how other disciplines relate to the readings and be prepared to discuss this aspect.

The assigned course readings will draw from a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans and strategies, and journals), implementation readings (government products that are responsive to or attempt to fulfill the requirements of authoritative documents), and external reviews (from the U.S. Government Accountability Office, Congressional Research Service, or other agency or office).

Access to and ability to use a library will be necessary for course completion and success. When possible, course readings are posted to CiteULike and, in many cases, are available from the DTIC web site. It is recommended that students become acquainted with their local public, university, or DoD (such as the Pentagon or NDU) library. In many cases, these institutions will allow library cardholders remote access to their databases and electronic publications.

Class participation is both important and required. The discussion forum is the classroom. If a student doesn't participate in the discussions on a weekly basis then that would be analogous to not showing up to class. As class participation is 25% of the grade (see below), failure to fully participate would make it nearly impossible to pass this course. If, due to an emergency, students are not able to respond to a discussion prompt in the week it is assigned, they must contact the instructor by e-mail and will be expected to post their response in the following week.

Weekly assignments must be posted in the Sakai CLE by midnight on the day they are due. It is expected that assignments will be submitted on time; however, it is recognized that students occasionally have serious problems that prevent work completion. If such a dilemma arises, students should contact the instructor before the assignment is due.

The completion of all readings assigned for the course is assumed. Since class will be structured around discussion, completion of the readings is crucial to support student participation in the class discussion forum. The majority of the class grade comes from participation and completion of the weekly assignments.

Each lesson will open on Sunday night at midnight and close the following Saturday at midnight. Forum participation (class discussion) must be completed by Saturday at midnight. If you elect to complete a weekly assignment (7 are due of the course of the semester) it must be turned in no later than midnight on Saturday.

Course Outline:

The following table outlines the 16-week course agenda. Graded assignments are in **bold**. Items in *italics* are ungraded but are required for a later, graded assignment.

Week	Topics	Instructional Method(s)	Student Assignments Due
1	Course Overview	• Reading • Asynchronous presentation • Discussion	• Discussion Forum: Introduction
2	Personnel Security Including cleared and un-cleared personnel	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 1**
3	Physical Security	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 2**
4	Information Security and Protection of unclassified information and OPSEC	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 3**
5	COMSEC and Information System Security	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 4**
6	Investigations	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 5**

Week	Topics	Instructional Method(s)	Student Assignments Due
7	Security Management	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 6** • *Midterm Exam Assigned*
8	Industrial Security and SAP/SAR and contracting	• Reading • Asynchronous presentation	• Discussion Forum • **Midterm Exam Due** • **Assignment 7**
9	Force Protection and Anti-Terrorism	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 8**
10	Nuclear Security	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 9**
11	Critical Infrastructure Protection and Cyber-security	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 10**
12	Acquisition Security and Research & Technology Protection	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 11**
13	Security Systems	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 12**
14	Integration and Interdependence of Security Disciplines	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 13**
15	Integration of Security Systems into Military Operations	• Reading • Asynchronous presentation • Discussion	• Discussion Forum • **Assignment 14** • *Final Exam Assigned*
16	Course Wrap Up/Future Trends and Issues	• Asynchronous presentation • Discussion	• Discussion Forum • **Final Exam Due**

Grading

The following provides a breakdown of how each assignment category to the overall performance in the class.

Category	Weight	Point Value
Class Participation	25%	250
Weekly Assignments	35%	350
Mid Term Exam	20%	200
Final Exam	20%	200
Total	**100%**	**1000**

A final letter grade will be assigned following the grading scale below:

Letter Grade	Point Range
A	900 -1000
B	800-899
C	700-799
D	600-699
F	599 and below

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.

Evaluation criteria for each graded assignment, including the midterm and final exams, 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.

It is expected that assignments reflect the original work of the student. In cases where the works of others are used it is expected that they will be appropriately attributed/cited in accordance with the Chicago Manual of Style. Assignments containing the works of others that are not properly attributed/cited will be returned ungraded. Failure to observe this policy can result in discipline from CDSE.

Assignment Evaluation Criteria					
	A Range	**B Range**	**C Range**	**D Range**	**F**
Content	Analysis and integration subject matter (readings, lecture, discussion, personal experience, etc.) is clear and convincing	Analysis and integration subject matter is clear and effective	Analysis and integration subject matter is underdeveloped	Analysis and integration subject matter is unsophisticated	Did not complete assignment
Organization	Paper shows exceptionally clear organization, purpose and focus	Paper shows good organization, purpose and focus	Paper lacks clear organization, purpose and focus	Paper is disorganized and confusing	
Grammar	Free of most grammatical errors	Some grammatical mistakes but generally shows successful grammar usage	Frequent grammatical errors	Appropriate grammatical knowledge not displayed for current language level	
Overall Effect	A strong overall effect with clear communication and support	A good overall effect with some support and adequate clarity	Paper struggles overall and does not give a coherent message	Paper has a poor overall effect and does not fulfill assignment	Did not complete assignment
Timeliness	Assignment turned in on time	Assignment turned in on time	Assignment turned in on time	Assignment turned in on time	

Class Participation (25%):

Participation includes completing all assigned readings, participating in the class discussion forum, participating in class exercises, and reflecting on the class experience. To achieve full credit for participation, students must **attend**, **participate**, and **reflect**. They must respond thoughtfully to all weekly discussion prompts, post responses to at least two other students' discussion posts each week, and provide constructive criticism when conducting peer reviews of other students' writing. Posts and responses should reflect a depth of critical thought and analysis on the subject at hand. Simply posting "I agree" or other such responses will not be deemed sufficient.

As mentioned earlier weekly participation in the on line discussion forum must be completed no later than midnight on the Saturday of the weekly lesson. Questions for discussion and participation requirements will be posted weekly in Sakai.

Weekly Assignments (35%):

There are fourteen weekly assignments. Students will be responsible for completing seven of these assignments during the course of the semester. Students are free to select which seven assignments they respond to. The topic for the written assignment should align to topic covered in the lecture and/or readings for the week(s) the student elects to turn in an assignment. For instance, if a student elects to write a paper in week 2 (which would be assignment 1) they should be writing on the subject(s) personnel security. Subsequent assignments (for a total of 7) follow the same guidance. The goal of the paper is to discuss/analyze an issue, problem or concern relating to the lesson topic. Students are expected to present solutions or recommendations in addition to discussing/analyzing the issue, problem or concern. Each assignment is worth 50 points for a total of 350 points for 7 assignments.

Produce a 500-1000 word (1-2 typewritten pages) critical analysis of the week's topic. The object of the assignment is to challenge student thinking on the subject and to develop new perspectives. Students are free to write the paper as they see fit, however they may want to consider one of the following approaches.

- Focus on how the readings relate to the week's lesson and how student experience(s) influence or impact the topic. It is not necessary to integrate all of the readings into the paper, but students can if they like.
- Write to one or more of the lesson's objectives and integrate any timely information and/or how the topic fits into the larger security realm writ large.
- Focus writing on an issue or problem in the topic of the week and describe how to approach addressing or fixing the issue/problem. It's not enough to talk about what's broken rather students should not only describe the problem but what steps need or should be taken to correct the problem

It is expected that written assignments reflect the original work of the student. In cases where the works of others are used it is expected that will be appropriately attributed/cited in accordance with the Chicago Manual of Style. Assignments containing the works of others that are not properly attributed/cited will be returned ungraded. Students may resubmit corrected assignments as long as they are received prior to the end of week 15.

Midterm Exam (20%):

The course midterm exam will be distributed in Week 8 and will be due during Week 9. It will cover material from Weeks 1 through 7 of class. The objective of the exam is to measure student performance relative to the course objectives. The midterm exam will consist of no more than five essay questions from which students will prepare three responses. Written communication, critical thinking skills, and integration of class material into the essay responses will demonstrate mastery of the subject.

The midterm exam will be graded using the pass/fail criteria noted above and/or other instructions provided to students for this exam.

(**IMPORTANT NOTE:** The objective of this exam is to gauge your knowledge and your thoughts on the subject at hand. Do not cut and paste large tracts of text from readings or other sources into your answers. Exams that include this type of information will be returned ungraded. If not corrected, a failing grade will be assigned. Next, fully read the question you are about to answer. In most cases it will be a multipart question. Ensure you answer all parts of the question)

Final Exam (20%):

The course final exam will be distributed in Week 15 and will be due during Week 16. The objective of the exam is to measure student performance relative to the course objectives. It will cover material from weeks 8 through 15 of class and will consist of no more than five essay questions from which students will prepare three responses. Written communication, critical thinking skills, and integration of class material into the essay responses will demonstrate mastery of the subject.

(**IMPORTANT NOTE:** The objective of this exam is to gauge your knowledge and your thoughts on the subject at hand. Do not cut and paste large tracts of text from readings or other sources into your answers. Exams that include this type of information will be returned ungraded. If not corrected, a failing grade will be assigned. Next, fully read the question you are about to answer. In most cases it will be a multipart question. Ensure you answer all parts of the question)

Course Textbooks

The bulk of the readings for this course will draw from a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans and strategies, and journals), implementation readings (government products that are responsive to or attempt to fulfill the requirements of authoritative documents), and external reviews (from the U.S. Government Accountability Office, Congressional Research Service, or other agency or office).

Supplemental readings may be selected from the following texts:

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011.

Sennewald, Charles A. *Effective Security Management, 5th Edition*. Boston: Elsevier Inc., 2011.

Additional But Not Required Texts for ED 501

Schneier, Bruce. *Beyond Fear. Thinking Sensibly About Security in an Uncertain World*. Springer, 2006.

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

Course Reading Assignments:

The following is an overview of the course reading assignments. Specific reading assignments will be in the lesson of the week posted on Sakai.

Lesson 1: Course Overview and Role of the Security Generalist:

Required Reading

Beaumont, Keaton L. "Developing 21st Century Senior Leaders," U.S. Army War College (2010). http://www.au.af.mil/au/awc/awcgate/army-usawc/dev_21c_leaders.pdf.

Bush, Charles D. "Logistics Generalist Development," U.S. Army War College (1987). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA180427.

Dror, Yehezkel. "Specialists vs. Generalists – A Mis Question." Rand Corporation (1968). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=AD0680695.

Lendaro, V. L. "A new Approach to Officer Development," Marine Corps Command and Staff College (2008). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA491610.

U.S. Department of Homeland Security. "TSA Success Profile." http://www.tsa.gov/assets/pdf/afsd_generalist_career_guide.pdf.

Additional Recommended Reading:

American Society for Industrial Security. "The ASIS Foundation Security Report: Scope and Emerging Trends." http://lepsc.org/documents/ASIS-Fndn-ScopeandEmergingTrends.pdf.

Drew, Christopher T. "Critical Thinking and the Development of Innovative Problem Solvers," Naval War College (2005). http://www.dtic.mil/cgi- bin/GetTRDoc?AD=ADA464378.

Kelly, Monroe. "Certifications for the Security Professional." http://bethanyduggan.wordpress.com/executive-protection-what-is-executive-protection/certifications-for-the-security-professional-by-monroe-kelly/.

Wilcock, Lawrence C. "Navy Intelligence Officer Detailing: A Case for Specialization." Marine Corps Command and Staff College (2010). http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA534928.

Lesson 2: Personnel Security:

Required Reading:

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapter 14.

Herbig, Katherine L. "Allegiance in a Time of Globalization." Defense Personnel Security Research Center (2008). http://www.dhra.mil/perserec/reports/tr08-10.pdf.

Herbig, Katherine L. "Changes in Espionage by Americans: 1947-2007." Defense Personnel Research Center (2008). http://www.fas.org/sgp/library/changes.pdf.

Heuer Jr., Richards J. and Janice L. Condo, "Summary and Explanation of Changes to the Adjudicative Guidelines Approved by the President December 29, 2005." Defense Personnel Security Research Center (2006). http://www.dhra.mil/perserec/reports/mr06-02.pdf.

Kramer, Lisa A., Richards J. Heuer Jr., and Kent S. Crawford. "Technological, Social and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage." Defense Personnel Research Center (2005). http://www.dhra.mil/perserec/reports/tr05-10.pdf.

Additional Recommended Reading:

Shaw, Eric D., and Lynn F. Fischer, "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations." Defense Personnel Security Research Center (2005). http://www.dhra.mil/perserec/reports/tr05-13.pdf.

Lesson 3: Physical Security:

Required Reading:

Department of Defense. ”Physical Security Program, 5200.8-R.” (2007). http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf.

Department of Defense. "Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control." (2009). http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-012.pdf.

Department of Homeland Security. "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors." (2004). http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1.

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapters 11 and 12.

Additional Recommended Reading:

Department of Defense Inspector General. "DoD IG Report to Congress on Section 357 of the National Defense Authorization Act for Fiscal Year 2008 Review of Physical Security of DoD Installations Report No. D-2009-035." (2009). http://www.dodig.mil/audit/reports/fy09/09-035.pdf.

Department of Defense Education Activity. “Internal Physical Security, DoDEA Regulation 4700.2.” (2001). http://www.dodea.edu/foia/iod/pdf/4700_2.pdf.

Department of Homeland Security. “Interagency Security Committee Use of Physical

Security Performance Measures.” (2009). http://www.dhs.gov/xlibrary/assets/isc_physical_security_performance_measures.pdf.

Lesson 4: Information Security:

Required Reading:

Department of Defense. ”Information Security Program and Protection of Sensitive Compartmented Information, 5200.1.” (2008). http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf.

Department of Defense. “DoD Operations Security (OPSEC) Program, 5205.02.” (2006). http://www.dtic.mil/whs/directives/corres/pdf/520502p.pdf.

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapter 21.

Federal Register. “Controlled Unclassified Information, Executive Order 13556.” (2010). http://www.archives.gov/isoo/policy-documents/eo-13556.pdf.

Liu, Edward C, and Todd Garvey. “Protecting Classified Information and the Rights of Criminal Defendants: The Classified Information Procedures Act.” Congressional Research Service (2011). http://assets.opencrs.com/rpts/R41742_20110331.pdf.

Lynch, Jennifer and Trevor Timm. “The Dangers in Classifying the News.” Electronic Frontier Foundation (October 2011). https://www.eff.org/deeplinks/2011/10/dangers-classifying-news.

Additional Recommended Reading:

None

Lesson 5: Information System Security:

Required Reading:

Department of Defense. “Information Assurance (IA) 8500.1E.” (2002). http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.

Department of Defense. “Communications Security (COMSEC), 8523.01. (2008). http://www.dtic.mil/whs/directives/corres/pdf/852301p.pdf.

Elmhirst, Sophie, “Bradley Manning, The Unknown Soldier.” New Statesman. (March 2011). http://www.newstatesman.com/north-america/2011/03/manning-house-held-base-iraq.

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapters 16 and 17.

Khatchadourian, Raffi. “No Secrets.” The New Yorker. (June 2010). http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian.

Additional Recommended Reading:

Department of Defense. “Management of the Department of Defense Information Enterprise 8000.1.” (2009). http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf.

Director of National Intelligence. “United States Intelligence Community Information Sharing Strategy.” 2008. http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf.

Luo, Xin and Merrill Warkentin. “Assessment of Information Security Spending and Costs of Failure.” Mississippi State University. http://www.information-institute.org/security/3rdConf/Proceedings/96.pdf.

The Joint Staff. “Joint Communications Systems, Joint Publication 6-0.” (2006). http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

Lesson 6: Investigations:

Required Reading:

Department of Defense. “Polygraph and Credibility Assessment Program, 5210.91” (2007). http://www.dodig.mil/Inspections/ipo/Pdfs/DoDD_5210.48.pdf .

Department of Defense. “Polygraph and Credibility Assessment Procedures, 5210.48.” (2010). http://www.dtic.mil/whs/directives/corres/pdf/521091p.pdf.

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapter 13.

Franey, Dave and Steve Seaton. Administrative Investigations.” (2008). http://www.cpms.osd.mil/ASSETS/65B4785282114B44BE51AA94D96280D9/Administratively%20Acceptable%20Evidence%20to%20Document%20Sick%20Leave.pdf.

Gilson, Bob. “Conducting Administrative Investigations and Writing Reports.” (2007). http://www.cpms.osd.mil/ASSETS/3BF55E95FAF846A887AAD96C277B7D7F/ConductingAdministrativeInvestigationsPrintVersion.pdf.

Navarro, Joe and John R. Schafer. “Detecting Deception.” FBI Law Enforcement Bulletin. (2001). http://www.au.af.mil/au/awc/awcgate/fbi/decep_detect_01.pdf.

Additional Recommended Reading:

Department of Justice. “Use of Polygraph Examinations in the Department of Justice.” (2006). http://www.fas.org/sgp/othergov/polygraph/dojpoly.pdf.

Naval Justice School. “JAGMAN Investigations Handbook.” (2001). http://www.imef.usmc.mil/mlg/specialstaffsections/SJA/investigations/JAGMAN%20INVESTIGATIONS%20HANDBOOK%20(Feb.%2001).pdf.

Navarro, Joe and John R. Schafer. “Detecting Deception.” FBI Law Enforcement Bulletin. (2001). http://www.au.af.mil/au/awc/awcgate/fbi/decep_detect_01.pdf.

Rossmo, D. Kim, “Criminal Investigative Failures.” Center for Geospatial Intelligence and Investigation, Department of Criminal Justice, Texas State University. (2005). http://www.justice.gov.sk.ca/milgaard/pubdocs/04262006/Kim%20Rossmo/337674.pdf.

Lesson 7: Security Management:

Required Reading:

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapters 3, 4 and 23..

Marine Corps Leadership Principles.” http://www.au.af.mil/au/awc/awcgate/usmc/leadership.htm.

Sennewald, Charles A. *Effective Security Management, 5th Edition*. Boston: Elsevier Inc, 2011. Chapters 1, 2, 3, 4 and 16.

Additional Recommended Reading:

Dess, Gregory G, G.T. Lumpkin and Marilyn L. Taylor. “Defining Strategic Management.” *Strategic Management. 2nd Edition.* New York: McGraw-Hill Irwin, 2005. http://www.sbaer.uca.edu/publications/strategic_management/pdf/01.pdf

Madden, Jerry. “100 Lessons Learned for Project Managers,” National Aeronautics and Space Administration. (2005). http://askmagazine.nasa.gov/issues/14/practices/ask14_lessons_madden.html.

Lesson 8: Industrial Security, Contracting and SAP/SAR:

Required Reading:

Department of Defense. “Joint Air Force, Army, Navy, Special Access Program Security Manual, JAFAN 6-0.” (2008). http://www.ncms-isp.org/documents/JANAF_6-0.pdf .

Department of Defense. “Special Access Program (SAP) Policy, 5205.07” (2010). http://www.dtic.mil/whs/directives/corres/pdf/520507p.pdf.

Department of Defense. “Directive-Type Memorandum (DTM) 09-019 – Policy Guidance for Foreign Ownership, Control, or Influence (FOCI).” (2009). http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-019.pdf.

Department of Defense. “National Industry Security Program Operating Manual (NISPOM), 5220.22M.” (2006). http://www.dss.mil/documents/odaa/nispom2006-5220.pdf.

Additional Recommended Reading:

Jackson, James K. “Foreign Investment, CFIUS, and Homeland Security: An Overview.” Congressional Research Service (2011). http://www.fas.org/sgp/crs/homesec/RS22863.pdf.

San Miguel, Joseph G. “Industrial Security Costs: An Analysis Of Reporting Practices.” Naval Postgraduate School (1993). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA272443.

Lesson 9: Force Protection and Antiterrorism:

Required Reading:

Department of the Air Force. Force Protection, Air Force Doctrine Document 3-10.” (2011). http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-10.pdf.

Department of Defense. “DoD Antiterrorism (AT) Program, 2000.12.” (2003). http://www.dtic.mil/whs/directives/corres/pdf/200012p.pdf.

Department of Defense. “DoD Antiterrorism (AT) Standards, 2000.16.” (2006). http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf.

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapter 25.

The Joint Staff. “Antiterrorism, Joint Publication 3-07.2.” (2010). http://www.bits.de/NRANEU/others/jp-doctrine/JP3_07.2(10).pdf.

Additional Recommended Reading:

Department of Defense. “Protecting the Force, Lessons from Fort Hood.” (2010). http://www.defense.gov/pubs/pdfs/DOD-ProtectingTheForce-Web_Security_HR_13jan10.pdf.

Department of Defense. “Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad.” (1996). http://www.dod.gov/pubs/downing_rpt/.

Department of Defense. Personal Accountability for Force Protection at Khobar Towers.” (1997). http://www.au.af.mil/au/awc/awcgate/khobar/cohen.htm.

Lesson 10: Nuclear Security:

Required Reading:

Department of the Air Force. “Command Directed Investigation, Concerning an Unauthorized Transfer of Nuclear Warheads Between Minot AFB, North Dakota and Barksdale AFB, Louisiana.” (2007). http://www.people.fas.harvard.edu/~jvaynman/Welcome_files/2.%20%20Commander%20Directed%20Investigation.pdf. (NOTE: report has been declassified and is redacted)

Department of the Air Force. “Blue Ribbon Review, Nuclear Weapons Policies and Procedures.” (2008). http://www.airforce-magazine.com/SiteCollectionDocuments/TheDocumentFile/Current%20Operations/BRR020808ExecSummary.pdf.

Department of Defense. Office of the Deputy Assistant to the Secretary of Defense for Nuclear Matters. “Nuclear Surety.” http://www.acq.osd.mil/ncbdp/nm/nuclearweaponssurety.html.

Schanz, Marc V and Suzann Chapman, “No More Bent Spears.” Air Force Magazine, 2008. http://www.airforce-magazine.com/Features/organization/Pages/box021508nuclear.aspx"

Spencer, Michael, Aadina Ludin and Heather Nelson. “The United States Air Force Minot and Taiwan Nuclear Weapons-Related Incidents: An Assessment.” Air University. (2011). http://www.au.af.mil/au/aul/school/awc/core/6200-15-spencer-united.pdf.

Additional Recommended Reading:

None

Lesson 11: Critical Infrastructure Protection (CIP) and Cyber-security

Required Reading:

Department of Defense. “Department of Defense Strategy for Operating in Cyberspace.” (2011). http://www.defense.gov/news/d20110714cyber.pdf.

Department of Homeland Security. “National Infrastructure Protection Plan.” (2009). http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapter 24.

McMillian, Robert. “Was Stuxnet Built to Attack Iran’s Nuclear Program?” PC World. (2010). http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

Morse, Eric S. “Homeland Security Gone Global.” The National Strategy Forum Review. (2011). http://nationalstrategy.com.dnnmax.com/Portals/0/documents/Winter%202011%20NSFR/Homeland%20Security%20Gone%20Global.pdf.

Moteff, John D. “Critical Infrastructures: Background, Policy and Implementation.” Congressional Research Service. (2009). https://www.dtic.mil/DOAC/document?document=ADA511284&collection=pub-tr&contentType=PDF&citationFormat=1f.

The White House. “The National Strategy to Secure Cyberspace.” (2003).

http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

Additional Recommended Reading:

Foster, John S., Jr, et.al. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report.” (2004). http://www.empcommission.org/docs/empc_exec_rpt.pdf.

Koning, Thomas L. "Proposed Supplemental Guidance for the Department of Defense's Critical Infrastructure Protection Plan." U.S. Army War College (2002). http://www.dtic.mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA401665.

Lesson 12: Acquisition Security and Research and Technology Protection:

Required Reading:

Department of Defense. Mandatory Procedures for Research and Technology Protection (RTP) Within The DoD, 5200.39-R." (Draft 2002). http://ebookpp.com/do/dod-5200.39-r-doc.html.

Department of Defense. "Critical Program Information (CPI) Protection Within the Department of Defense, 5200.39." (2008). http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf.

Department of Defense. "Acquisition Systems Program Protection, 5200.1M." (1994). http://www.dtic.mil/whs/directives/corres/pdf/520001m.pdf.

Department of Defense. "Program Protection Plan Outline & Guidance." (2011). http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf.

Fay, John J. *Contemporary Security Management, 3rd Edition*. Boston: Elsevier Inc, 2011. Chapter 5.

Office of the Director, Defense Research Engineering/Systems Engineering. "Acquisition Security Related Policies and Issuances." (2009). https://acc.dau.mil/adl/en-US/302946/file/45529/acq-security-policy-tool-text.pdf.

Additional Recommended Reading:

Bartlett III, James Ellwood. *The Annotated ITAR.* 2011.

http://www.ndia.org/Resources/ExportImportComplianceResources/Documents/Annotated%20ITAR%20(6%20Dec%2011).pdf

Bureau of Industry and Security, U.S. Department of Commerce. Export Administration Downloadable Files. http://www.bis.doc.gov/policiesandregulations/ear/index.htm.

Department of Defense. "Defense Acquisition System, 5000.01." (2002). http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.

Department of Defense. "National Industry Security Program Operating Manual (NISPOM), 5220.22M." (2006). http://www.dss.mil/documents/odaa/nispom2006-5220.pdf.

Department of Defense. "Operation of the Defense Acquisition System, 5000.02." (2008). http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf.

Defense Security Service. "Self-Inspection Handbook for NISP Contractors." (2008). http://www.dss.mil/seta/documents/self_inspect_handbook_nisp_08.pdf.

Duke, Elaine. “Why Acquisition Programs Fail – And What to do About It.” HSToday 2010). http://www.hstoday.us/channels/dhs/single-article-page/why-acquisition-programs-fail-and-what-to-do-about-it/c43e8c4852e009da20993b2f093b4c89.html.

Lesson 13: Security Systems:

Required Reading:

Department of Defense. “Military Handbook Design Guidelines for Physical Security of Facilities MIL-HDBK 1013/1A.” (1993). https://portal.navfac.navy.mil/portal/page/portal/NAVFAC/NAVFAC_WW_PP/NAVFAC_NFESC_PP/LOCKS/PDF_FILES/MIL-HDBK-1013-01A.pdf

Department of Defense. “Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E), 3224.03.” (2007). http://www.dtic.mil/whs/directives/corres/pdf/322403p.pdf.

Department of Defense. “Physical Security Program, 5200.08R.” (2007). http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf.

The Joint Staff. “Joint Operations in the Theater, Joint Publication 3-10.” (2010). http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf. Chapter 4.

Additional Recommended Reading:

None

Lesson 14: Integration and Interdependence of Security Systems:

Required Reading:

Baker, Sharon L. “Managing Resistance to Change.” Library Trends Vol 38, no. 1 (1989) pp 53-61. http://www.ideals.illinois.edu/bitstream/handle/2142/7649/librarytrendsv38i1h_opt.pdf?sequence=1.

Department of the Air Force. “Information Protection CONOPS.” (2008)

Fay, John J. *Contemporary Security Management, 5th Edition*. Boston: Elsevier Inc., 2011. Chapters 7 and 8.

Sennewald, Charles A. *Effective Security Management, 3rd Edition*. Boston: Elsevier Inc., 2011. Chapter 23.

Additional Recommended Reading:

None.

Lesson 15: Integration of Security Systems into Military Operations:

Required Reading:

Lafrenz, James L. "Doctrine (Maybe), Strategy (No), Will the Air Force Implement a Force Protection Program?" Air War College Maxwell Paper No. 12. (1999). http://www.au.af.mil/au/awc/awcgate/maxwell/mp17.pdf.

The Joint Staff. "Joint Security Operations in Theater, Joint Publication 3-10." (2010). http://www.dtic.mil/doctrine/new_pubs/jp3_10.pdf.

Additional Recommended Reading:

Tzu, Sun. *The Art of War*. trans. Lionel Giles.

http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf.

Lesson 16: Course Wrap Up/Future Trends and Issues:

Required Reading:

None

Additional Recommended Reading:

None