Cybersecurity and Oversight of Information System Security (CDSE ED 514)

Defense Security Service (DSS)
Center for Development of Security Excellence (CDSE)
Education Division

SAMPLE COURSE SYLLABUS*

1 Course Description/Overview

The ability to secure information within a modern enterprise—large or small—is a growing challenge. Threats to information security are global, persistent, and increasingly sophisticated. Long gone are the days when managers could hope to secure the enterprise through ad hoc means.

Effective information security at the enterprise level requires participation, planning, and practice. It is an ongoing effort that requires management and staff to work together from the same script. Fortunately, the information security community has developed a variety of resources, methods, and best practices to help modern enterprises address the challenge. Unfortunately, employing these tools demands a high degree of commitment, understanding, and skill—attributes that must be sustained through constant awareness and training.

It is important to note as well that effective security is not achieved in stovepipes. Ineffective physical security, for example, can undermine otherwise effective information system security, and vice versa. Effective security at the enterprise level requires the effective interaction of physical security, information security, personnel security, and so on—indeed, all branches of security must interact effectively as a system to achieve overall enterprise security.

This course is designed to teach mid-level security practitioners how to engage all functional levels within the enterprise to deliver information system security. To this end, the course addresses a range of topics, each of which is vital to securing the modern enterprise. These topics include *inter alia* plans and policies, enterprise roles, security metrics, risk management, standards and regulations, physical security, and business continuity. Each piece of the puzzle must be in place for the enterprise to achieve its security goals; adversaries will invariably find and exploit weak links.

Additionally, the Department of Defense (DoD) is itself a massive enterprise, and security practitioners should understand the context and importance of their activities within the overall DoD enterprise. To this end, the course will emphasize the practical implications of cybersecurity management to DoD roles and missions through the application and study of timely examples.

2 Target Audience/Prerequisites

This course is intended for DoD civilian and military personnel who perform security leadership and management duties. All students will be required to have achieved the Security

*Sample syllabus is subject to change each semester.

Fundamentals Professional Certification (SFPC) under the DoD Security Professional Education Development Program (SPēD) or to have comparable fundamental knowledge of DoD security programs.

3 Student Outcomes/Objectives

At the end of this course, students will be expected to be able to:

- Assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures;
- Critique and assess the strengths and weaknesses of general cybersecurity models, including the CIA triad;
- Appraise the interrelationships among elements that comprise a modern security system, including hardware, software, policies, and people;
- Assess how all domains of security interact to achieve effective system-wide security at the enterprise level.
- Compare the interrelationships among security roles and responsibilities in a modern information-driven enterprise—to include interrelationships across security domains (IT, physical, classification, personnel, and so on);
- Assess the role of strategy and policy in determining the success of information security;
- Estimate the possible consequences of misaligning enterprise strategy, security policy, and security plans;
- Design a notional information security plan that incorporates relevant principles of lifecycle management;
- Evaluate the principles of risk and conduct a notional risk management exercise;
- Assess the role of good metrics and key performance indicators (KPIs) in security assessment and governance;
- Create a good set of information security metrics;
- Critique the current legal and regulatory environment as it applies to cybersecurity;
- Identify and contrast the most common security standards and associated catalogues of security controls;
- Contrast the various approaches to security training and formulate a simple training agenda;
- Justify the need for business continuity planning and propose how to implement such a plan successfully within a modern enterprise;
- Compare and contrast logical and physical security;
- Appraise the current structure of cybersecurity roles across the DoD enterprise, including the roles and responsibilities of the relevant organizations;
- Assess the strengths and weaknesses of the certification and accreditation approach to cybersecurity;
- Evaluate the trends and patterns that will determine the future state of cybersecurity.

4 Delivery Method

This is a graduate-level distance-learning course in assessing current and future security functions, technologies, and systems relevant to DoD programs. The course will consist of readings, lectures and presentations, asynchronous sessions, participation in the discussion forum, graded research papers, and three quizzes.

Because this is a 3 credit hour equivalent course, the contact time over the 16 weeks should be approximately 30 hours. A typical week will include a 45–60 minute lecture or equivalent presentation with notes and comments; the lecture or presentation will be followed by either a quiz (about one hour duration to complete), an alternative assignment, or an on-line discussion forum. Generally a discussion will be based on instructor-provided discussion question(s) with each student providing a response and then commenting on other student inputs. This discussion format will constitute the remainder of the contact time for each lesson (for eight lessons).

Students should be prepared to discuss and debate the readings as well as examine and assess them for biases and multiple perspectives. Students should also be investigating 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). Students will be provided with a large number of open access and password protected sites yielding a tremendous number of peer-reviewed research assets.

Students will also be expected to monitor and interpret current information security news and will be provided with links to news stories and events during the course. These will help support the structured online discussions.

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. Students will also receive information for signing on to approximately a dozen other research sites or databases relevant to security and defense studies; one example would be 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 (such as the Pentagon and NDU libraries).

5 General Course Requirements

Class participation is both important and required. If, due to an emergency, students are not able to respond to a discussion promptly 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 2359 EST 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 in a timely fashion.

6 Academic Integrity Policy

"The Center for Development of Security Excellence holds its students, faculty, and staff to the highest standards of integrity and security. The Center does not tolerate the misleading use of any information and data. All alleged violations of academic integrity will be investigated and resolved.

Violations Defined: The CDSE specifically prohibits cheating, plagiarism, and the toleration of those students who do.

Cheating is defined as committing an act with the intent to receive undeserved credit or gain an unfair advantage, or assisting, or attempting to assist, others in doing likewise.

Plagiarism is defined as the act of taking ideas, writings, or the like from another and passing them off as one's own by not providing the proper credit to the original author. Specifically, it is the intentional, knowing, or reckless failure to document or correctly attribute another's ideas.

Plagiarism includes, but is not limited to:

The duplication of an author's words without both quotation marks and accurate references or footnotes and/or use of an author's ideas in paraphrase without accurate reference or footnotes.

Students are expected to credit properly and accurately the source of materials directly cited or indirectly used (i.e., paraphrased) in any oral or written work. All student work shall be their own, unless otherwise properly noted.

Toleration is defined as a student or students believing that a violation of academic integrity may have occurred and not reporting the violation. Any student who knowingly witnesses a violation of academic integrity and does not report the same will be considered as having committed a cheating or plagiarism violation."

7 Grading

The following provides an approximate breakdown of how each assignment contributes to the overall performance in the class.

Class participation (via online discussion)	15%
Quizzes	15%
Final exam	20%

Research paper	30%
Security Project	20%

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

A = 90% – 100%
B = 80% – 89%
C = 70% – 79%
D = 60% – 69%
F = 59% 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 discussion question responses are listed below.

ASSIGNMENT EVALUATION CRITERIA
• Uses complete sentences • Uses proper grammar structure
• Responses reflect depth of thought and critical thinking skills
• Integrates material from class/readings into responses
• Provides coherent and reasoned responses to all questions
• Integrates real world examples into responses
• Meets submission timeline

Evaluation criteria for each graded assignment aside from discussion questions, 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.

Assignment Evaluation Criteria					
	A	**B**	**C**	**D**	**F**
Content	Analysis and interpretation 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	

Assignment Evaluation Criteria					
	A	**B**	**C**	**D**	**F**
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	Did not complete assignment
Overall Effect	A strong overall effect with clear communication and peer-level support	A good overall effect with 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	
Timeliness	Assignment turned in on time	Assignment turned in on time	Assignment turned in on time	Assignment turned in on time	

Class Participation (15%):

To meet the requirement for sufficient contact time each week, there will be a combination of presentations and lectures by the instructor along with online discussions by and among the students. This approach will be true for eight of the lessons. In a typical weekly lesson, the presentation and notes require a minimum student engagement of 45 minutes (the student can absorb the presentation in smaller periods if desired). The students will then be presented one or two discussion questions for response to the instructor and then comment on the inputs from two other students. Each of these eight online discussions is worth 20 points. The student response to the instructor is worth 4 or 8 points. Each comment to a fellow student is worth 3 or 6 points. The time expected to complete this online response/comment is one hour.

Quizzes (15%):

Each quiz will be the equivalent of one hour of contact time and together will be worth fifteen percent of the overall grade. The quizzes will be short answer (choosing five out of seven questions). The first quiz will cover material covered up to that point in the course. The second quiz will cover material covered since the first quiz.

Final Exam (20%):

The final exam will assess the students' ability to critique, assess, and apply the principles and topics presented during the course. While the two quizzes (above) will require the students to answer a set of short questions, the final exam will require the students to answer two questions in depth (five pages each, double spaced, for a total of 10 pages, not including bibliography). Students will be expected to document their sources and will be required to employ the *Chicago Manual of Style* as the exam's style and citation guide.

Research Paper (30%):

The students will be required to write a graduate-level research paper (20 pages, double spaced, not including front matter and bibliography). The paper will allow the students to delve more deeply into the challenges of managing the systems that help assure the confidentiality, integrity, and availability of information. Outside research will be required, and the students will be required to employ the *Chicago Manual of Style* as the paper's style and citation guide.

Students will deliver the paper in three phases: (1) an annotated bibliography of sources documented using *Chicago* style, (2) a draft of the completed paper, and (3) a final version of the paper. This phased approach will allow the instructor to provide students with feedback along the way instead of only at the end of the project. Overall, the students will be required to evaluate the topic with an eye toward defending and justifying a well-reasoned position.

Security Project (20%)

In the security project, each student will prepare a *notional* security plan and *notional* risk assessment (approximately 10 pages, double spaced, not including the risk assessment spreadsheet). This plan will address the issues discussed in the texts and the course and tailor the plan to a context defined by the student. This risk assessment will be built using MITRE's Risk Matrix tool. It will reflect real-world conditions but not represent a real-world system or enterprise. The student will be expected to apply a superior level of analysis when creating the combined plan. As with the research paper, students will be required to employ the *Chicago Manual of Style* as the paper's style and citation guide.

8 Course Evaluation

You will have the opportunity to evaluate the course several different ways throughout the semester. You will have access to post your feedback to a forum through Sakai. The forum will remain open throughout the semester, and it will be monitored regularly. Participation in the forum is entirely optional. You will also complete two online course evaluations: one at the middle of the semester and one after the semester. As this is the first time we've offered this course, your experience and feedback is invaluable to our ability to improve the course for future CDSE students.

9 Course Textbooks

The following texts will serve as the primary resources for this course:

- Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition, . *Information Sec Management*: *Concepts and Practice*. New York, McGraw-Hill, 2013.
- Whitman, Michael E. and Herbert J. Mattord. *Roadmap to Information Security for IT and Infosec Managers*. Boston, MA: Course Technology, 2011.

Students must purchase or otherwise obtain these two texts for this course.

10 Course Outline

The following table outlines the 16-week course agenda.

Week	Topics	Method of instruction	Assignments due
1	The Security Environment • Threats, vulnerabilities, and consequences • Advanced persistent threats • The state of security today • Why security matters to DoD	• Reading • Presentation with notes and comments	Student introductions
2	Principles of Cybersecurity • The interrelated components of the computing environment • Cybersecurity models (the CIA triad, the star model, the Parkerian hexad) • Variations on a theme: computer security, information security, and information assurance	• Reading • Presentation with notes and comments • Discussion	Discussion forum (DF) 1: Respond to instructor discussion questions and other student responses
3	Cybersecurity Management Concepts • Security governance • Management models, roles, and functions	• Reading • Presentation with notes and comments • Discussion	DF 2
4	Enterprise Roles and Structures • Information security roles and positions • Alternative enterprise structures and interfaces	• Reading • Presentation with notes and comments	Annotated bibliography
5	Strategy and Strategic Planning • Strategy • Strategic planning and security strategy • The information security lifecycle • Architecting the enterprise	• Reading • Presentation with notes and comments • Discussion	DF 3
6	Security Plans and Policies • Levels of planning • Planning misalignment • The System Security Plan (SSP) • Policy development and implementation	• Reading • Presentation with notes and comments • Discussion	Quiz 1

Week	Topics	Method of instruction	Assignments due
7	Laws and Regulatory Requirements • Timeline of U.S. laws related to information security • The Federal Information Security Management Act (FISMA)	• Reading • Presentation with notes and comments • Discussion	DF 4
8	Security Standards and Controls • Security standards and controls • Certification and accreditation (C&A)	• Reading • Presentation with notes and comments	Research paper (draft)
9	Risk Management • Principles of risk • Types of risk • Risk strategies • The Risk Management Framework (RMF)	• Reading • Presentation with notes and comments • Discussion	DF 5
10	Security Metrics and Key Performance Indicators (KPIs) • The challenge of security metrics • What makes a good metric • Approaches to security metrics • Metrics and FISMA	• Reading • Presentation with notes and comments	Research paper (final version)
11	Physical Security and Environmental Events • Physical and environmental threats • Physical and environmental controls	• Reading • Presentation with notes and comments • Discussion	DF 6
12	Contingency Planning • Developing a contingency plan • Understanding the different types of contingency plan • Responding to events	• Reading • Presentation with notes and comments • Discussion	Quiz 2
13	Security Education, Training, and Awareness • Human factors in security • Developing and implementing a security training plan • Cross-domain training (IT and other security domains)	• Reading • Presentation with notes and comments • Discussion	DF 7

Week	Topics	Method of instruction	Assignments due
14	Managing information security across the DoD enterprise (1) • The purpose of certification and accreditation • Trends in certification and accreditation	• Reading • Presentation with notes and comments • Discussion	Security project
15	Managing information security across the DoD enterprise (2) • The strategic direction of DoD IT and information security • Responsibilities within the DoD enterprise	• Reading • Presentation with notes and comments • Discussion	DF 8
16	The future of cybersecurity • Key future uncertainties • Possible future scenarios • How to apply what you've learned	• Reading • Presentation with notes and comments	Final exam