The Future of Security Systems and Information Assurance
(CDSE ED 510)

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

SAMPLE COURSE SYLLABUS*

1 Course Description/Overview

It is commonly and correctly observed that the flow of information has expanded greatly since the 1990s. In parallel, our dependence on this flow has deepened, as has the need to secure it from exploitation, theft, and denial. The ability to assure the confidentiality, integrity, and availability of our information was always important—today, however, it is essential.

It is vital to note that the domain of information assurance is in a state of flux. New threats and threat vectors emerge regularly, and defenses are required to adjust accordingly. The task of capturing the current and future state of information assurance is akin to the task of capturing the state of radar and electronic warfare in 1940. A student of the domain must therefore understand both the underlying principles, which remain relatively stable, and the more dynamic patterns of attack and defense that emerge through a constant flow of security events. The key, of course, is to anticipate these patterns and get ahead of the attacker.

Persons responsible for designing, implementing, and operating information systems, then, must start with a solid understanding the core principles of information assurance, information security, and security engineering. In short, they need to know what to secure and how to secure it. This in turn requires them to understand principles of risk, governance, knowledge management and sharing, and systems engineering.

Students in the course will be required to evaluate principles and applications in each of these areas, with an overall emphasis on operative security systems. The course will first introduce students to the necessary conceptual and analytical framework. This framework will include an overview of the current security environment and a review of the risks and opportunities inherent in this environment. A key concept here is the notion of tradeoffs—every new system introduces both opportunities and risks, and sometimes neither the opportunities nor the risks are immediately apparent. Students will be given a toolkit of analytical methods for structuring their understanding of these systems and will be required to model systems using this toolkit.

This background will give students the ability to properly contextualize the functions and design tradeoffs of operative security systems. Students will be introduced to each system of interest and its associated functions and properties. (It is worth noting that this is not a course in software or systems engineering, although principles of both apply.)

Students will be expected to critique the general principles and analytical toolkit introduced during the course to the effort of evaluating the risks and opportunities associated with the

*Sample syllabus is subject to change each semester.

systems of interest. They will also be expected to synthesize practical lessons and heuristics across the body of systems addressed. Students will be expected to exhibit this analysis and synthesis in both online discussions and the research projects, particularly the second project, which will require them to design a notional future security system that performs one or more of the critical functions discussed during the course.

The course will close by considering the future of security systems. This is a necessary coda; the security environment changes rapidly, and security professionals must attempt to anticipate these changes. The pre-recorded lectures, readings, and assignments completed during the course should enable the students to engage in a healthy and informed evaluation of the factors driving the future security environment and the possible effects of changes within that environment.

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.

2 Target Audience/Prerequisites

This course is intended for DoD civilian and military personnel who perform security leadership and management duties. It is assumed that all students will be prepared to take on graduate-level work in the security field.

3 Student Outcomes/Objectives

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

- Assess the current security environment, including the risks and opportunities that attend new processes and technologies;
- Summarize the nature and role of information assurance in both providing and protecting information;
- Evaluate the essential issues involved in sharing and protecting information, including issues of risk, knowledge sharing, and education;
- Appraise the interrelationships among elements that comprise a modern security system, including hardware, software, policies, and people;
- Differentiate the functions and types of modern security systems and illustrate them using specific examples;
- Assess the tradeoffs that security engineers should consider when designing, implementing, and operating balanced security systems;
- Evaluate the factors and issues that frame the possible future security environments, and estimate the effect of these issues on current security design and operations;
- Examine and assess the roles, responsibilities, requirements, and effectiveness of select DoD information systems and programs;
  - Investigate and evaluate the effectiveness of information assurance relative to the DoD Information Assurance Certification and Accreditation Process (DIACAP);

  - Discuss and evaluate the effectiveness of how information assurance principles are applied in the National Industrial Security Program (NISP);
  - Discuss and evaluate the security effectiveness of information systems that currently exist to support DoD security programs; and
- Appraise information systems that could or should be developed in the future (near-term and long-term) to support DoD security.

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 and interprets 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	
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 open-book 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 interpret, critique, and assess, and 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 primary text for this course will be Jason Andress' *The Basics of Information Security*, published by Syngress in 2011. This continues to be one of the most concise introductions to the topic. Mark Rhodes-Ousley's *Information Security, The Complete Reference*, Second Edition (2013) complements the material in the Andress volume by providing additional information on specific topics. Students must purchase or otherwise obtain these two texts for this course.

10 Course Outline

Week	Topics	Method of instruction	Assignments due
1	Overview of the Security Environment • Course and student introductions • The state of information assurance today • Advanced persistent threats • Why information assurance (IA) matters at DoD	• Reading • Asynchronous presentation and interaction	Student introductions/ biographical sketch.
2	Transitioning to the Future—Cloud and Mobile Computing • Cloud computing • Mobile computing systems • Bring-your-own-device (BYOD) policies	• Reading • Asynchronous presentation • Discussion	Discussion forum (DF) 1: Respond to instructor discussion questions and other student responses
3	Transitioning to the Future—Social Media • Social media • Information sharing	• Reading • Asynchronous presentation • Discussion	DF 2
4	Risk Analysis • Understanding system-wide tradeoffs • Risk strategies • Risk management	• Reading • Asynchronous presentation • Discussion	Annotated bibliography
5	Systems Engineering and Security • Systems engineering concepts • Systems and enterprise architecture • Security metrics	• Reading • Asynchronous presentation • Discussion	DF3

Week	Topics	Method of instruction	Assignments due
6	The Human Side of Security • The psychology of security • Social engineering • The insider threat • Security education and knowledge sharing	• Reading • Asynchronous presentation	Quiz 1
7	IA Concepts I • Identification and authentication • Authorization and access control • Auditing and accountability	• Reading • Asynchronous presentation • Discussion	DF4
8	IA Concepts II • Cryptography • Operations security • Physical security	• Reading • Asynchronous presentation	Research paper (draft)
9	IA Concepts III • Network security • Operating system (OS) security • Application security	• Reading • Asynchronous presentation • Discussion	DF 5
10	Systems and Programs I: IA in DoD Practice • Legislation, compliance, and legal issues • Roles, responsibilities, and requirements • DIACAP	• Reading • Asynchronous presentation • Discussion	Research paper (final version)
11	Systems and Programs II: NISP • Roles, responsibilities, functions, and requirements • NISPOM	• Reading • Asynchronous presentation • Discussion	DF 6
12	Systems and Programs III: Information Systems Supporting Security Programs • Programs and systems (JPAS, DCII, SWFT, etc.) • Introduction to Security Project	• Reading • Asynchronous presentation • Discussion	Quiz 2

Week	Topics	Method of instruction	Assignments due
13	Analysis Toolkit I • Summary discussion of systems from session 12 • Scenario planning: why, what, how • Further discussion of Security Project	• Reading • Asynchronous presentation • Discussion	• DF 7
14	Analysis Toolkit II • Scenario planning • Future security technologies	• Reading • Asynchronous presentation	Security project
15	Critical review of student papers (security project draft, phase II) on security system models and possible future security systems.	• Reading • Asynchronous presentation • Discussion	DF 8
16	Wrap-up • Key lessons and principles • Future trends and constraints • How to apply what you've learned	• Reading • Asynchronous presentation	Final exam