

COLLEGE OF PROFESSIONAL STUDIES
Professional Security Studies Department-Undergraduate
SECU 422

1. **Abbreviated Course Title:** COMPUTER SECURITY III
2. **Full Course Title:** Computer Security III - Advanced
3. **Credits:** Three (3) undergraduate degree credits, 45 contact hours with additional study/activities expected outside the classroom.
4. **Catalog Description:** This capstone course focuses on the importance of information security (INFOSEC) and the impact technology has in the field of security. Major domains covered are National Training Standard for Information Systems Security – (NSTISS) planning/management, and policies/procedures. Specific topics include: security planning, risk management, systems lifecycle management, contingency planning/disaster recovery, physical security measures, personal security practices and procedures, software security, network security, administrative controls, auditing, cryptosecurity, key management, transmission and TEMPEST security.
5. **Course Prerequisites:** SECU 322 – Computer Security II or permission of instructor.
6. **Rationale:** Students typically enter this course with an intermediate level of computer security knowledge. Everyone is expected to continually self-reflect on the ways computers and associated technology can improve professional practice. The foci of the course are to review or learn the fundamentals of computer security, create a knowledge base, and maximize day-to-day applications for the professional security field. By design, this course will build upon following three thinking skills:
 - knowledge
 - comprehension
 - application, using the terminology, hands-on, and references provided throughout this course.

And develop the top three cognitive areas of Bloom’s Taxonomy:

 - analysis
 - synthesis, and
 - evaluation.

Students are expected to become proficient with the use of the technology to communicate with their respective professional communities in meeting their duties and responsibilities.
7. **Student Learning Outcomes and Course Goals:** Students who successfully complete this course will be able to...
 - A. INTEGRATE NSTISS requirements into security planning.
 - B. EMPLOY risk management techniques.
 - C. DESIGN and EVALUATE systems lifecycle management aspects for security planning and management.

- D. EXPLAIN contingency planning/disaster recovery operations.
- E. DISCUSS practical performance measures in designing security measures
- F. INTRODUCE generic security planning guidelines and documentation
- G. IDENTIFY physical security measures.
- H. SEPARATE personal security practices and procedures.
- I. APPLY software security.
- J. PRACTICE network security.
- K. ASSEMBLE administrative security procedural controls.
- L. COMBINE auditing and monitoring.
- M. ORGANIZE elements of vulnerability and threat that exist in a given AIS/telecommunication system with corresponding protection measures.
- N. CONSTRUCT specific technological, policy and educational solutions for NSTISS.
- O. PRIORITIZE cryptosecurity and key management.
- P. ASSESS transmission security.
- Q. SUPPORT Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) security.
- R. DEVELOP a personalized webliography through the use of a self-reflective journal from personal learning obtained in this course.
- S. DETERMINE which resources are best.
- T. REFLECT on the impact of computer security.

8. Instructional Procedures:

- Hands-on computer use (encourages student engagement)
- Lecture (minimal – designed to invoke thought and reflection)
- Group discussion and interaction
- Individual assignments/projects
- Student presentations of their computer security webliography

9. Course Content:

UNIT	TOPIC	SUBTOPICS	OUTCOMES
1	Security Planning	NSTISS policy; NSTISS program budget; NSTISS program evaluation; NSTISS training	A, R, S, T
2	Risk Management	Accreditation; Corrective Actions; Information Identification; Risk Analysis/Evaluation	A, B, R, S, T
3	Systems Lifecycle Management	Acquisition; Design Review and Systems Testing; Security Specification; Application Sensitivity; Management Control Process; Systems	A, B, C, R, S, T

		Certification	
4	Contingency Planning/Disaster Recovery	Continuity of Operations; Contingency Plan Components; Backup Requirements; Recovery Actions; Offsite Processing; Emergency Destruction; Critical and Essential Guidelines; Team Response Responsibilities	A, B, C, D, R, S, T
5	Physical Security Measures	Alarms; Building Construction; Cabling; Communication Centers; Environmental Controls; Filtered Power; Information System Centers; Physical Access control; Power Controls; Protected Distributed Systems; Shielding; Standalone System and Peripherals; Storage Area Controls	E, F, G, R, S, T
6	Personal Security Practices and Procedures	Need to Know; Contractors; Employee Clearances; Position Sensitivity; Security Training and Awareness; Systems Maintenance Personnel	E, F, H, R, S, T
7	Software Security	Change Controls; Documentation; Access Privileges; Audit Trails and Logging; Concept of Least Privilege; Identification and Authentication; Internal Labeling; Malicious Logic Protection; Need to Know Controls; Operating Systems Security Features; Segregation of Duties	E, F, I, R, S, T
8	Mid-term Examination		A through I
9	Network Security	Dialup vs. Dedicated; End-to-End Access Control; Class/Nodes; Public vs. Private; Traffic Analysis	J, R, S, T
10	Administrative Security Procedural Controls	Attribution; Construction and Changing; Copyright;	K, R, S, T

		Destruction of Media; Documentation; Emergency Destruction; External Marking of Media; Media downgrading and declassification; Security Plans; Computer misuse/abuse; Repudiation; Media Sanitization; Media Transportation	
11	Auditing and Monitoring	Security Reviews; Security Program Effectiveness; Investigation of Breaches; Monitoring Systems; Privacy; Accountability Controls; Audit Logs and Trails; Software Design Standards; Testing and Evaluation	L, R, S, T
12	Cryptosecurity and Key Management	Cryptovvariable/Key; Electronic Key Management; Encryption/Decryption Method/Procedure; COMSEC Access, Storage and Control; COMSEC Destruction; COMSEC inventory/identification; Protocols; Reporting Incidents	M, N, O, R, S, T
13	Transmission Security	Burst Transmission; Cross Talk; Dial Back; Directional Signals; Frequency Hopping; Jamming; Line-of-Sight; Line Authentication; Low Power; Masking; Optical Systems; Protected Wireline; Screening; Spread Spectrum Transmission	M, N, P, R, S, T
14	TEMPEST Security	Attenuation; Banding; Cabling; Filtered Power; Grounding; Shielding; TEMPEST Separation; Zoning	M, N, Q, R, S, T
15	Final Examination		A through Q

Due to the nature of IA/Cyber Security courses, use of personal computers and University computer labs are **REQUIRED**. See CITI and computer lab links:

<http://www.njcu.edu/programs/citi/>
<http://www.njcu.edu/ac/home.htm>
<http://www.njcu.edu/ac/labs/proflabs.htm>

10. Undergraduate General Studies Courses: Not applicable – this is a College of Professional Studies offering/free elective.

11. Graduate Course Status: Not applicable – undergraduate level course.

12. Programmatic/Departmental Outcomes:

Programmatic: This course fulfills the mission of the College of Professional Studies to provide students with the knowledge, skills and abilities in the professions to:

- Become lifelong learners for personal and professional enrichment
- Be effective and productive leaders and/or managers in their respective professional careers

Departmental: The development of this free elective allows all Professional Security Studies majors to meet the elective requirements while maintaining a direct connection to the field. The Department is committed to this *scholar-practitioner* approach. This course is part of a deliberate three-course sequence needed for computer security professionals.

13. Degree Requirements: This course is a free elective.

14. Specialized Accreditation, Certification, and Licensure: This course in conjunction with SECU 222 and 322 has been mapped against the *National Security Agency's (NSA)* certification requirements for *National Training Standard for Information Systems Security (INFOSEC) for Professionals – NSTISS 4011*. Certain aspects of this permanent course approval request are designed to comply with the *NSA* standards, i.e. course names, proficiency levels, universal references and increasing content (covering 256 elements), over the entire three course sequence. Levels are aligned with the course levels, e.g. SECU 222 - Basic = “novice,” SECU 322 - Intermediate = “apprentice,” and SECU 422 - Advanced = “proficient.” In other words, upon successful completion of the appropriate courses/student learning outcomes, our students would be rated at these levels within the field of Information Security (INFOSEC).

In addition to internal University evaluation, these courses have been externally reviewed by National level Information Assurance subject matter experts and determined to meet the *NSTISS 4011* standard. *New Jersey City University* received

National recognition from the *NSA* along with certification for these three courses on June 5, 2007.

15. Assessment/Evaluation of Student Outcomes and Determining Student Grades:
a. Describe how students will be assessed on an ongoing basis and how their performance will be evaluated. Describe examinations, term or research papers, special projects, class performance, seminar presentations, and portfolios in relation to student learning outcomes (Item 7). Include type of examination, nature of papers and projects, etc.

Students will be continuously assessed throughout the semester with regular detailed and prompt feedback in keeping with modern assessment concepts. The following sets forth the assessment/evaluation tool being used and the nature of the assignment(s) used to evaluate student outcomes:

ASSESSMENT/EVALUATION TOOL	NATURE OF ASSIGNMENTS USED TO EVALUATE STUDENT OUTCOMES
Class Participation	-Personal observations of in-class computer use -Class discussions of assigned readings -Presentation of group responses to issues discussed in each class
Exams	-Written essay examinations for mid-term and final examination
Oral Presentations	-Individual presentation of one selected advanced-level computer security topic
Webliography	-Individual creation of a list of 20 computer security resources available on the Internet

b. Please indicate the percentage assigned to each assessment/evaluation tool.

ASSESSMENT/EVALUATION TOOL	% OF TOTAL GRADE	OUTCOMES
Class Participation	20 %	A through Q
Midterm Exam	20 %	A through I
Oral Presentation	10 %	J through Q
Final Exam	30 %	A through Q
Self-Reflection Journal	10 %	A through T
Webliography	10 %	A through Q

16. References (APA format):

a. Required Text(s):

Pfleeger, C. P. & Pfleeger, S. L. (2006). *Security in Computing (4th Ed.)*. Upper Saddle River, NJ : Prentice Hall, 2006.

Department of Commerce, National Institute of Standards and Technology. (1995) *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook*. Available on-line at:

<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>.

Washington, DC: author.

Additional Required Resources: IA/Cyber Security Education Resources and Links for central access point for all historical documents (THESE ARE REQUIRED FOR ALL IA/CYBER SECURITY COURSES!!!):

<http://web.njcu.edu/sites/profstudies/securitystudies/Content/links.asp>

b. Supporting Bibliography: (See the following:)

*Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ: John Wiley and Sons, Inc.

*Biery, K. & Hager, D. (2001). *The Risks of Mobile Communications*. New Jersey City University, NJ, Proquest Web site:
<http://proquest.umi.com/pqdweb?did=955777295&Fmt=3&clientId=44872&ROT=309&VName=PQD>.

Bishop, M. (2003). *Computer Security: Art and Science*. Upper Saddle River, NJ: Pearson Education, Inc.

Clarke R. (2000). *An Artefact Ill-Fitted to the Needs of the Information Society*.
<http://www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html>

Curtin, M. (2001). *Developing Trust: Online Privacy and Security*. Berkeley, CA: Apress LP.

Denning, D. (1982). *Cryptography and Data Security*. Cartersville, MA: Addison-Wesley.

Easttom, C. (2006). *Computer Security Fundamentals*. Upper Saddle River, N.J.: Pearson Prentice Hall.

*Gollmann, D. (2006). *Computer Security (2nd ed.)*. Hoboken, NJ: John Wiley and Sons, Inc.

- Hamilton, P. (1972). *Computer security*. Philadelphia, PA: Auerbach Publishers.
(Reference is added to demonstrate this subject is not as new as many students may believe; the text is available from the Library of Congress).
- Internet Security Systems, Inc. (2000). *Microsoft Windows 2000 Security Technical Reference*. Redmond, WA: Microsoft Press.
- *Karygiannis, T. & Owens, L. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices*. Washington, DC: Technology Administration, US Department of Commerce.
- Kenigsberg, N. et al. (2004). *A Framework for HIPAA IT Security Compliance: Leveraging for Security*. Washington, DC: EDUCAUSE Center for Applied Research Bulletin.
- *LaMacchia, B. et al. (2002). *.NET Framework Security*. New York: Addison Wesley Longman, Inc.
- *National Institute of Standards and Technology. (2005). *Special Publication 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Washington, DC: author.
- National Security Agency. (1994) *National Training Standard for Information Systems Security (INFOSEC) for Professionals – NSTISS 4011*. Washington, D.C.: author.
- *Neumann, P. (1995). *Computer-Related Risks*. Cartersville, MA: Addison-Wesley.
- *Russell, D. & Gangemi, Sr., G. (1991). *Computer Security Basics*. Sebastopol, UK: O'Reilly and Associates.
- *Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ: John Wiley and Sons. Inc.
- Zwicky, E. et al. (2000). *Building Internet Firewalls, 2nd Edition*. Sebastopol, UK: O'Reilly & Associates.

NSA References –Government Reference Format

- [CHR90]Interview with Agent Jim Christy, Chief, Air Force Office of Special Investigations, Computer Crime Division, 26 March 1990.
- [DOD85]*Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Department of Defense, Washington, DC, December 1985.

[DOJ88] *Basic Considerations in Investigating and Proving Computer-Related Federal Crimes*, U.S. Department of Justice, Justice Management Division, Washington, DC, November 1988.

[HIG89] Higgins, John C., "Information Security as a Topic in Undergraduate Education of Computer Scientists," *Proceedings of the 12th National Computer Security Conference*, November 1989.

[MAC89] Maconachy, W.V., "Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation into Practical Reality," *Proceedings of the 12th National Computer Security Conference*, November 1989.

*[OTA87] U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310, Washington, DC, U.S. Government Printing Office, October 1987.

*[PFL89] Pfleeger, Charles P., *Security in Computing*, Prentice-Hall, 1989.

Note - * = holdings physically present in the *Congressman Frank J. Guarini Library*. Other resources are available through inter-library loan(s). All resources have been validated and available at the U.S. Library of Congress at: <http://www.loc.gov>

c. Relevant Periodical Sources:

Computer Fraud & Security (2002 – Present)
Computer Security Update (1999 – Present)
Information Systems Security (1995 – Present)
Journal of Computer Security (1996 – Present)
Security Dialogue (2001 – Present)

All of the above journals/periodicals can be accessed through the EBSCO Academic Search Premier:
<http://www.njcu.edu/guarini/clicktracker/click.asp?id=128&ky=>
 (Requires GothicNet ID)

d. Relevant Online Materials (if not noted above):

American Society for Industrial Security, International: www.asisonline.org
 Computer Security Organizations: www.sans.org
 Federal Bureau of Investigation: www.fbi.gov
 Improving CyberSecurity Research in the United States:
www7.nationalacademies.org/cstb/project_cybersecurity.html
 Journal of Security Administrators: www.wiu.edu/users/mfkac/jsa
 National Security Agency: www.nsa.gov
 Society of Competitive Intelligence Professionals: www.scip.org
 Department's Webpage: www.njcu.edu/professionalsecurity

17. Enrollment and Scheduling: This course will be routinely offered (each regular semester – Fall and Spring, along with selected Summer sessions each year) with a minimum of 10 students and a maximum of 25* per class.

* - some computer labs only have 22 stations and that would be the maximum if assigned less than 25 computers.

18. Resources:

- a. Supplies & Materials: A computer lab that allows each student to individually have hands-on activity throughout the course. Other items that would assist with delivery are Smart Board and/or projector for power point, blackboard, chalk and erasers.
- b. Equipment:
 - 1.) Smart board and/or projector for power point.
 - 2.) Dedicated Information Technology Classroom.
- c. Space Allocation: No additional space required.

19. Budget: The department's current budget covers all costs.