Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

# A University Course in Information System Risk Analysis / Security Certification and Accreditation

N. Paul Schembari, Ph.D., East Stroudsburg University of Pennsylvania

***Abstract*—The East Stroudsburg University of Pennsylvania course "Risk Analysis / Certification and Accreditation" is offered as a model for implementation of NSTISSI 4015 – the National Training Standard for System Certifiers. The experiences of the instructors in teaching this course are illustrated.**

**Index Terms— Education, Computer Security, Information Assurance, Security Planning, Risk Analysis, Security Certification and Accreditation**

## I. Introduction

As more universities enter into the field of information assurance (IA) education, they look for standards in the field. One place to find such standards is from *the Committee for National Security Systems* (CNSS) *Instructions Web Site* [1]. One of the CNSS Standards covers curriculum concerning the security certification and accreditation of information systems – CNSS 4015: *National Training Standard for System Certifiers* [2]. At East Stroudsburg University of Pennsylvania (ESU), we have developed our course Computer Science (CPSC) 326: *Risk Analysis / Certification and Accreditation* to help our students meet this standard.

For those unfamiliar with the terminology of *Security Certification and Accreditation of Information Systems*, we will use the following definitions:

- *Risk* = A measure of the probability and the impact (consequences) of threats/attacks to information systems;
- *Risk Analysis / Assessment* = The determination and measurement of risk to information systems;
- *Security Certification* = An assessment of the threats, vulnerabilities, and controls of an information system with regard to the system's security requirements;
- *Security Accreditation* = Senior management authorization for the operation of an information system based on the results of security certification and risk assessment;
- *C&A* = The process of performing a security certification which leads to a security accreditation of an information system.

One easily found source for information on the C&A process for federal systems is the *NIST FISMA Implementation Project* [3]. FISMA is the *Federal Information Security Management Act* of 2002 [4] which tasked the US Department of Commerce to create a "suite of security standards and guidelines required by the legislation as well as other FISMA-related publications necessary to create a robust information security program and effectively manage risk to agency operations and agency assets." [5]

It should be noted that while FISMA requires the C&A process for all federal systems which are not *National Security Systems*[*], a robust C&A program is a good recommendation for any information system. In fact, the *Sarbanes-Oxley Act* of 2002 [6] places requirements on

*N. Paul Schembari is a Professor of Computer Science and Computer Security at East Stroudsburg University of Pennsylvania and the Director of the University's Computer Security Program.*

[*] A *National Security System* is defined in FISMA as an information system whose function, operation, or use

- involves intelligence activities,
- involves cryptologic activities related to national security,
- involves command and control of military forces,
- involves equipment that is an integral part of a weapon or weapons system,
- is critical to the direct fulfillment of military or intelligence missions, or
- involves classified information in the interest of national defense or foreign policy.

ISBN 1-933510-98-6/$15.00 © 2006 CISSE 

the information systems of publicly-held companies that are similar to the FISMA requirements.

Because of the extensive documentation which is available online for the FISMA Implementation Project [3] we have chosen this methodology as the basis for CPSC 326 at ESU.

In this paper, we will present an overview of our CPSC 326 course, analyze the FISMA Implementation Project from a pedagogical point of view, and illustrate our experiences in teaching this course.

## II. C&A IN THE ESU CURRICULUM

CPSC 326: *Risk Analysis / Certification and Accreditation* is a junior level course, typically taken by about twenty to twenty-five students per year. As an IA prerequisite, students are first required to complete our IA overview course CPSC 325: *Fundamentals of Security Engineering* before they take CPSC 326 so that they have a good background before learning C&A and risk analysis. The students are introduced to C&A in CPSC 325, but at an awareness level only. CPSC 326 has been designed to give students an understanding of C&A at the performance level.

Since the students in CPSC 326 are typically junior Computer Security majors, they have also completed extensive coursework in computer science including Introductory Programming, Linear and Non-Linear Data Structures, Computer Organization, and Operating Systems Concepts and Design. They have also completed courses in mathematics - Calculus, Discrete Mathematics, and Probability and Statistics are required for the major and the students should have completed most of these classes by the time they take CPSC 326.

The students will also have completed general education coursework outside of their majors, but an analysis of these classes and their major classes shows that CPSC 325 and 326 are the first classes in which students are engaged with system management. Since system management is taught at only the awareness level in CPSC 325, the first course for our students in system management at a performance level is CPSC 326, our Risk Analysis / C&A course. We will address these issues further in Section V. *Lessons Learned* below.

While completing CPSC 326, some students may also take our required *Applied Network Security* course where they experiment with some tools in the field. Other students complete *Applied Network Security* in their senior years. Computer Security majors finish their major requirements with courses in *Applied Computer Cryptography*, *Legal Impacts in Computer Security Solutions*, and the *Security Engineering Internship*. During the internship course, where students are employed and earn credit, similar to a "co-op" program, some students have applied the skills and information gained from CPSC 326 to help in the performance of a C&A of a federal system. For further information, visit the ESU Computer Security Program website [7], or access our description of the ESU program at CISSE 2005 [8].

## III. NIST FISMA IMPLEMENTATION PROJECT OVERVIEW

The FISMA Implementation Project is a result of the E-Government Act of 2002 [9]; FISMA is Title III of the E-Government Act. FISMA requires federal agencies to develop security plans for their systems, assign security responsibilities, and perform security certifications and security accreditations on their systems. NIST is responsible for first creating guidelines for this process.

The NIST guidelines are distributed as Federal Information Processing Standards (FIPS) or NIST Special Publications (SP) in the "800 series." The entire 800 series of special publications are available on the NIST website [10], and besides providing information for the FISMA implementation, they also give good overall IA information. The FIPS and SP that apply to FISMA are available on the FISMA Implementation Project Library Page [11]. As of March 2006, this library page also contained Microsoft PowerPoint presentations which gave an overview of C&A, a strategy for agencies to apply the FISMA provisions, and a FIPS update. Third, links to legislation, policies, and directives which apply to FISMA implementation are also included on this page.

Let us now consider the FISMA Implementation documents which apply directly to the ESU CPSC 326 course. We do not reference most of the documents directly as they are all available from the FISMA Implementation Project Library Page [11].

- FIPS 199*, Standards for Security Categorization of Federal Information and Information Systems*, gives direction on defining a "risk level" for an information system. These levels are "high", "moderate", or "low" based on the security factors confidentiality, integrity, and availability.
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, is intended to be used in conjunction with FIPS 199 to help in the determination of the risk level of a system.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is currently in draft form, and gives a brief description

of the least robust security requirements required for federal systems. As an example, the requirement "Identification and Authentication" is described as "Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems." [12, p. 3]

- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, illustrates the process of developing a system security plan for either major applications or general support systems. The suggested plan includes sections on system identification, management controls, operational controls, and technical controls. Also, many templates which follow 800-18 are available online; for example, the US Department of Housing and Urban Development has a template available for Major Applications [13].
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, outlines the entire C&A process. This guide shows the preparation needed for a C&A, the fine aspects of certification and accreditation, and the details of the post-accreditation phase for systems.
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, shows how security controls map to the security requirements of FIPS 200. It also outlines how these controls must apply to Low, Moderate, and High risk systems as defined in FIPS 199. For easier viewing, the controls which are recommended for each risk level are also broken down in three annexes. As an example, consider the control "Access Enforcement" which is defined as "The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy." [14, p. 41]
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, is currently in draft form, and provides methods for testing the security controls given in SP 800-53. For example, one method to test the "Access Enforcement" control given above is to "Examine access control mechanism to determine if the information system is configured to implement the organizational access control policy." [15, p. 43]

The FISMA Implementation Project Library page includes more documents than those given above, but we only include these since they are the publications included in the CPSC 326 course.

It is clear from this brief overview that the FISMA Implementation Project has succeeded in its goals of creating guidelines to address the provisions of FISMA: federal agencies must develop security plans for their systems, assign security responsibilities, and perform security certifications and security accreditations on their systems. With this extensive documentation, it is also clear that we have an excellent resource for a university course in risk analysis / security certification and accreditation.

## IV. The ESU Risk Analysis / C&A Course

Let us now consider the details of the ESU course CPSC 326: *Risk Analysis / Certification and Accreditation*. The course objectives include:

- To give students knowledge of security planning at the performance level in accordance with U.S. government standards;
- To give students a broader and deeper understanding of assessing vulnerabilities in accordance with U.S. government standards;
- To provide students a practical instruction in the process of collecting data, analyzing computer risks, and producing an assessment and corrective recommendations in contemporary computer systems;
- To teach essential concepts, algorithms, and protocols of applied information assurance and operational availability.

In order to achieve these objectives, we provide students with classroom discussions on security planning and C&A, have the students perform in-class and homework exercises, and have students build a security plan and perform major portions of the C&A process on a live information system.

### *A. Introduction*

We begin the course with an overview of risk analysis and assessment and C&A. The students have been exposed to these topics in our CPSC 325: *Fundamentals of Security Engineering* course, so we now include more detail. With regard to Risk Analysis and Assessment, we introduce some basic methodologies for calculating risk, all based on the probabilistic idea of *expectation*. Some of this overview material is based on Chapter 8 of Pfleeger's text, *Security in Computing* [16]. In class exercises illustrate how *residual risk* (the risk that remains after a control is implemented) can be determined. For homework exercises, the students are asked to determine a number of threats to a college information system, and then estimate the probability that these threats becomes attacks, and the impact (cost) of the attacks. Data is collected from each student and aggregated in a Delphi approach.

To continue the introductory materials we also discuss C&A, and especially the FISMA Implementation Project. The students are given an overview to the documentation discussed in Section III. above, and of the laws and mandates which affect C&A, some of which are historical. We discuss the Computer Security Act, the IT Management Reform Act, Government Information Security Reform Act, FISMA, Office of Management and Budget Circular A-130, Appendix III, Homeland Security Presidential Directive #7, and the Sarbanes-Oxley Act.

The students are also given more detail on C&A during this introductory material. They learn the essential documentation that is required – the security plan, the "certification package", and the "accreditation package". They also learn the roles of the various individuals involved; for example, how the System Owner must create the security plan with the help of the Information Systems Security Officer, and then get this plan approved by the Designated Approving Authority (DAA). Later in the process, the Certifying Agent and the System Owner prepare the certification package for the DAA, and the DAA uses this information to make the accreditation decision. Details such as these are expanded for the students.

### *B. Security Planning*

With the completion of the introductory material, the course moves onto the topic of "Security Planning". Here, we follow NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, described in Section III. above. The students are shown how to determine the correct information for each section of the required security plan. In class, we discuss how we would complete the plan for various portions of campus - typically "The Computer Science Department". Then, the students are broken into groups of four or five, assigned a student computer laboratory on campus, and required to complete portions of the plan for this system. Since the students are not allowed full disclosure of required information for these systems from the campus administration, we only require that the students complete a portion of the plan. The required sections from NIST SP 800-18 are given below, and not all items in these sections are required because of the students lack of knowledge. Also, for the same reason, some entire sections required by 800-18 have been omitted.

0) Plan Control
1) System Identification
    a) System Name/Title
    b) Responsible Organization
    c) Information Contacts
    d) Assignment of Security Responsibility
    e) System Operational Status
    f) General Description/Purpose
    g) System Environment / Architecture / Topology
    h) System Interconnection/Information Sharing
    i) Sensitivity of Information Handled
    j) Laws, Regulations, and Policies Affecting the System
2) Management Controls
    a) Review of Security Controls
    b) Rules of Behavior
3) Operational Controls
    a) Personnel Controls
    b) Physical and Environmental Protection
    c) Production, Input/Output Controls
    d) Hardware and System Software Maintenance Controls
    e) Integrity Controls
    f) Documentation
4) Technical Controls
    a) Identification and Authentication
    b) Logical Access Controls
    c) Audit Trails

The plans that the student teams create are considered learning exercises. They are graded in an effort to be sure that the teams will provide the correct information for the second security plan they will develop. This second plan involves the certification and accreditation exercise, so we discuss this in Section IV. C. below.

It should be noted that other important planning and policy documents are also discussed as part of this course. These include Rules of Behavior (or Acceptable Use Policies), Business Continuity Plans, and Incident Response Plans. Other important topics are the determination of system security requirements and the determination of system risk level, where we use FIPS 199, FIPS 200, and NIST SP 800-60.

### *C. Certification, Risk Assessment, and Accreditation "in the Classroom"*

After the in-class discussion on security planning, and while the students are working on their campus lab security plan exercises, we move onto the specifics of C&A. In class, we cover the ideas presented in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. With these discussions, the students learn how to perform a certification, what the "baseline" controls should be for federal information systems, how to assess these controls, and how accreditation occurs.

Besides discussion, the best experience for the students is to perform a certification. To allow the students this opportunity, a certification site is arranged for the class. We have typically used campus facilities with which the students are not familiar (for example, the ESU Center for Research and Economic Development), or local high school facilities. The instructor coordinates the certification with the appropriate administrators of the facilities and also decomposes the system into subsystems. In this way, one student team may be evaluating a single computer lab, or a small office complex, or a few high school classrooms each of which has a few workstations. Unless the class is particularly large, each team investigates a unique portion of the system.

Because of the possible sensitivity of the information at these facilities, the students are once again not given full access. Also the site visits by the students and any testing is supervised by the instructor. No penetration testing from off-site is performed. As with the security plan exercise mentioned in Section IV. B. above, this lack of access for the student teams implies that they cannot provide a complete certification and accreditation. Below are the sections from NIST SP 800-37 which the students are required to complete. Some of these requirements also show notes that have been given to the students. The numbering system used gives the required tasks and subtasks from NIST SP 800-37; for example, Task 1 is "Preparation" and Subtask 1.1 is "System Description". The students are required to complete the following subtasks to the best of their abilities with the restrictions set forth above:

Task 1 Preparation
1.1 System Description – Follow 800-37 and 800-18
1.2 Security Categorization – Follow FIPS 199
1.3 Threat Identification
1.4 Security Control Identification – Follow 800-53
1.5 Vulnerability Identification
Task 2 Notification and Resource Identification
2.2 Planning and Resources – C & A Plan
Task 4 Security Control Verification
4.1 Documentation and Supporting Materials
4.2 Reuse of Evaluation Results – For similar hardware/software
4.3 Techniques and Procedures – Design security tests and use 800-53A
4.4 Security Evaluation
4.5 Security Test and Evaluation Report
Task 5 Security Certification Documentation
5.1 Certification Findings and Recommendations
5.2 Security Plan Update – Create final Security Plan
5.3 Security Certification Package Assembly
Task 6 Security Accreditation Decision
6.1 Residual Risk Determination (Actual)
6.2 Residual Risk Acceptability
Task 7 Security Accreditation Documentation
7.1 Accreditation Package Transmission – Just the Accreditation Letter based on 6.1 and 6.2
Task 9 Ongoing Security Control Verification
9.1 Security Control Selection – Make recommendations

A few comments regarding the required subtasks, and those not required, are in order.

- Task 1 allows the students to create most of the required security plan, which can be updated as they proceed through the C&A process.
- Subtask 1.6 is "Residual Risk Determination (Expected)" and is not included for the students. Here, the system owner is supposed to determine what residual risk they believe will remain in the system based on the current controls. The students perform this analysis in Subtask 6.1.
- Subtask 2.2 is one of the first required documents – the students are asked to outline how they will complete the C&A.
- Subtask 2.1 is "Notification" and is not included for the students. Here, appropriate parties are informed that the certification will commence. This is not necessary for our class exercise.
- Task 3 is "Security Plan Analysis, Update, Acceptance" and not included for the students. The students are asked to complete a final security plan in Subtask 5.2.
- Task 6 – the student teams are required to compute risk based on statistical expectation and using the Delphi data from Section IV. A. above (which they are allowed to modify).
- Subtask 7.1 – the student teams are required to act as the Designated Approving Authority and determine if the system they have reviewed should be granted "Full Authorization to Operate", "Interim Approval to Operate", or "Denial of Authorization to Operate" as defined in the C&A process.
- Subtask 7.2 is "Security Plan Update " and not included for the students. The students are asked to complete a final security plan in Subtask 5.2.
- Task 8 is "Configuration Management and Control" and not included for the students. The students cannot be involved in this process, but can make recommendations on policies regarding configuration management and control.
- Subtask 9.2 is "Security Control Monitoring" and not included for the students. The class cannot be involved in this process, but are required to make recommendations on what controls should be monitored and the frequency of the monitoring.

- Task 10 is "Status Reporting and Documentation" and not included for the students. The class cannot be involved in this process, but can make recommendations on what should be reported and the frequency of these reports.

We believe that this partial certification and accreditation, along with the development of two security plans gives our students a good introduction to Risk Analysis, Certification and Accreditation of Information Systems, and Security Planning and Management.

## V. Lessons Learned

The ESU CPSC 326: *Risk Analysis / Certification and Accreditation* course has been offered many times, and the instructors have developed multiple techniques and overcome obstacles for this course. We now consider some of the insights gained by the instructors. In particular, we will discuss available resources for a course like CPSC 326, how students react to their first experiences in system management, issues involved with coordinating the certification of an off-campus system, and experiences with the typical student assignments in CPSC 326.

### *A. Textbooks and Course Resources*

A variety of resources exist to help with the instruction of a course like CPSC 326. For the first two iterations of the course, the instructors tried Peltier's *Information Security Risk Analysis* [17]. However, most of this material was deemed unnecessary for the course. In fact, in the second iteration, the material from Peltier that was deemed necessary was discussed in about three hours of lecture.

A relatively new book is *Security Assessment* by Miles, et al [18]. Instead of working with C&A, this book deals with the NSA INFOSEC Assurance Methodology [19]. However, this methodology is not enough to satisfy the requirements for C&A. As described by Miles, et al [18, p. xxxi], "An assessment can be part of a certification, but it does not provide a proper level of assurance in and of itself because it does not contain hands-on testing." In fact, to accompany the IAM, the NSA has the corresponding INFOSEC Evaluation Methodology [20] which provides more hands-on evaluations. A text in this area would be highly desirable.

Other books on security assessments are available, but most do not address C&A. However, very recently (December 2005), a new C&A book has been published: *Building and Implementing a Security Certification and Accreditation Program* by Patrick Howard [21]. We are in the process of reviewing this text for use in our course.

Of course, with the NIST publishing much documentation on C&A as related to FISMA, an instructor may decide to offer a C&A course without a text book. In fact, in the last two iterations of the ESU C&A course, no text has been used with success. However, instructors should be aware that the FISMA Implementation resources [11] are quite extensive, and much effort will be involved in streamlining these resources into a workable course.

Besides the FISMA Implementation Project Library which has been used for our course, we should also mention two other government sources. For those interested in following the *US Department of Defense IT Security Certification and Accreditation Process* (DITSCAP), documentation is available on the DITSCAP website [22]. Our students are given this site as a reference. Note that DITSCAP will soon be replaced with DIACAP - *US Department of Defense Information Assurance Certification and Accreditation Process*. The third government resource for C&A is the *National Information Assurance Certification and Accreditation Process* which is available to the public from the Committee for National Security Systems [23]. The NIACAP differs from the FISMA Implementation Project in that "The National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 6 establishes the requirement for federal departments and agencies to implement a C&A process for national security systems under their operational control." [23, p. 2] That is, NIACAP is meant for national security systems. It should be noted that there is much overlap between all three federal programs.

### *B. Students' First Courses in System Management*

As mentioned in Section II. above, our CPSC 325 and CPSC 326 courses are the first courses where students learn some topics of system management. Our instructors have found this transition to be a challenge for students, especially with regard to student expectations. We have found that the students believe that IA coursework should be mostly technical. In fact, since our program is based in our Computer Science Department, some students feel that our IA coursework should focus on the development of security tools. While we do help students learn many aspects of security software development, our program is intended to give students a broad background in IA which should, of course, also include an understanding of IA management and operational methods.

Our solution to address this issue has been two-fold. First, our instructors have made an effort to inform students on the goals of our program and inform them on their typical duties when they graduate and become employed. Some students will be involved with development, but others will work in the less technical

aspects of the field. Many students learn of this dual role of the security engineer as they work on their internships. A second solution to this problem has been to allow students to learn from practitioners. One of our adjunct instructors is President and CEO of a local computer security firm, and the students' interaction with him has allowed them to learn the multiple aspects of the field. We have also invited IA professionals to campus as part of our Colloquium series to give the students more of the practitioner's point of view.

One interesting point on student expectations is that we have found (anecdotally) that students who come with some experience in the field before they complete our coursework do agree with our mutual emphasis on software development and non-technical issues.

### C. Coordinating the C&A

One of the most difficult aspects of the course for the instructor is the coordination of the C&A with an outside organization. As mentioned in Section IV.C. above, we have typically used local high schools or campus sites with which the students are less familiar. The more difficult sites are those off-campus, the local high schools. East Stroudsburg University and our Computer Science Department work on many joint projects with our local high schools, and therefore, we have many contacts. Using our contacts, especially with school district technology directors, we have offered our services as a "free security review of your facility".

In most cases, the technology directors have been interested in this service (especially if they have been under recent attack), but getting approval from their administration might be problematic. In order to get approval, we have typically given guarantees such as no penetration testing from outside the organization, the students will be monitored by faculty, the students must sign a code of conduct, etc. As should be expected, the school administration must be made comfortable about the process, and we always have a good discussion on ethics and conduct with our students.

Another issue is the fact that these technology directors / system administrators are busy with their normal duties, and they are really providing a volunteer service to allow our class on their facility. Of course, they do get the certification and accreditation package as a final product to help evaluate their system security, but they must make time to interface with our class. Because of these time restrictions, we have typically performed on-site analysis in a limited fashion. The instructor will have one or two introductory meetings to overview the system and analyze it for system decomposition, and then the class will meet at the facility for its first site visit. Here we typically perform a physical inspection of the facility. Then, each student team schedules a time to perform on-site testing of their sub-system together with both the instructor and the system administrator. In the end, each student team is on site for about three to four hours.

We also have used automated vulnerability scanning and surveying techniques to help us gather information about the certification site. This information is provided to the student teams to include in their final documentation, and the vulnerability scanning is performed on a "typical" workstation for the facility with the assumption that other workstations have similar configurations. This is also done to minimize to time we spend on-site.

### D. Student Assignments

For the ESU CPSC 326 course, the student assignments consist of the compilation of threats to a campus information system, including probability and impacts, the creation of a security plan for a campus subsystem, and then the creation of a security plan, the partial certification, and the partial accreditation of an off-site information system. We believe that these assignments give our students a good background in the C&A and Risk Analysis processes.

As was mentioned in Section V.B. above, this course is one of the students' first in system management. For this reason, we have found that the students require much direction in the required document creation. While our students do complete a course in *Technical Writing*, offered by our English Department, this is a general course, and the specifics of Security Plans, Security Test and Evaluation Reports, etc., are difficult for our novice security engineers. The students' need for direction in writing Security Plans has been corroborated at other universities; for example, see Clark's paper "The Security Plan: Effectively Teaching How to Write One" [24].

## VI. CONCLUSION

The East Stroudsburg University course CPSC 326: *Risk Analysis / Certification and Accreditation* has been successfully offered since 2001 to more than 100 students. The course gives our students an understanding of risk analysis, security certification, and accreditation of information systems. Our course follows the FISMA Implementation Project to perform a partial C&A of a live system. Furthermore, we believe that it may be possible to use this course to help our students earn the National Training Standard for System Certifiers (NSTISSI 4015) certification. We have mapped our curriculum to this standard, have submitted our application to the Committee on National Security Systems, and at the time of this writing, await their decision.

## VII. REFERENCES

[1] Committee for National Security Systems; *CNSS Instructions*; Retrieved on March 9, 2006 from http://www.cnss.gov/instructions.html.

[2] National Security Telecommunications and Information Systems Security Committee; *National Training Standard for System Certifiers (NSTISSI 4015)*; Retrieved on March 9, 2006 from http://www.cnss.gov/Assets/pdf/nstissi_4015.pdf

[3] National Institute of Standards and Technology; *FISMA Implementation Project*; Retrieved on March 9, 2006 from http://csrc.nist.gov/sec-cert/.

[4] One-Hundred Eighth Congress of the United States of America; *Federal Information Security Management Act of 2002*; Retrieved on March 9, 2006 from http://csrc.nist.gov/policies/FISMA-final.pdf.

[5] National Institute of Standards and Technology; *FISMA Implementation Project –Project Phases*; Retrieved on March 9, 2006 from http://csrc.nist.gov/sec-cert/ca-proj-phases.html

[6] One-Hundred Eighth Congress of the United States of America; *Sarbanes-Oxley Act of 2002*; Retrieved on March 9, 2006 from http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:%20

[7] East Stroudsburg University; *East Stroudsburg University Center for Computer Security and Information Assurance*; Retrieved on March 9, 2006 from http://www.esu.edu/compusec/

[8] Schembari, N. Paul; "A Bachelor of Science Degree in Computer Security: The Experiences of a National Center of Academic Excellence in Information Assurance Education"; *Proceedings from the Ninth Colloquium for Information Systems Security Education*, 2005, pp. 6 – 11.

[9] One-Hundred Eighth Congress of the United States of America; *E-Government Act of 2002*; Retrieved on March 9, 2006 from http://csrc.nist.gov/policies/HR2458-final.pdf

[10] National Institute of Standards and Technology; *NIST Special Publications*; Retrieved on March 9, 2006 from http://csrc.nist.gov/publications/nistpubs/

[11] National Institute of Standards and Technology; *FISMA Implementation Project - Library*; Retrieved on March 9, 2006 from http://csrc.nist.gov/sec-cert/ca-library.html

[12] National Institute of Standards and Technology; *Federal Information Processing Standard 200, Minimum Security Requirements for Federal Information and Information Systems,* Initial Public Draft; Retrieved on March 9, 2006 from http://csrc.nist.gov/publications/drafts/FIPS-200-ipd-07-13-2005.pdf

[13] U.S. Department of Housing and Urban Development; *Major Application System Security Plan*; Retrieved on March 9, 2006 from http://www.hud.gov/offices/cio/sdm/devlife/tempchecks/mastemplate.doc

[14] Ross, Ron, et al; *NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems*; Retrieved on March 9, 2006 from http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

[15] Ross, Ron, et al; *NIST Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems,* Initial Public Draft; Retrieved on March 9, 2006 from http://csrc.nist.gov/publications/drafts/sp800-53A-ipd.pdf

[16] Pfleeger, Charles P. and Pfleeger, Shari L.; *Security in Computing*, Third Edition; Prentice Hall Publishing, Upper Saddle River, NJ, 2003.

[17] Peltier, Thomas R.; *Information Security Risk Analysis*; Auerbach Publishing, Boca Raton, FL, 2001.

[18] Miles, Greg, et al; *Security Assessment: Case Studies for Implementing the NSA IAM*; Syngress Publishing, Rockland, MA, 2004.

[19] National Security Agency; *INFOSEC Assurance Methodology Homepage*; Retrieved on March 9, 2006 from http://www.iatrp.com/iam.cfm.

[20] National Security Agency; *INFOSEC Evaluation Methodology Homepage*; Retrieved on March 9, 2006 from http://www.iatrp.com/iem.cfm.

[21] Howard, Patrick D.; *Building and Implementing a Security Certification and Accreditation Program*; Auerbach Publishing, Boca Raton, FL, 2005.

[22] US Department of Defense; *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*; Retrieved on March 9, 2006 from http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf.

[23] US National Security Telecommunications and Information Systems Security Committee; *National Information Assurance Certification and Accreditation Process (NIACAP)*; Retrieved on March 9, 2006 from http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

[24] Clark, Paul C.; *The Security Plan: Effectively Teaching How To Write One*; Retrieved on March 9, 2006 from http://cisr.nps.navy.mil/downloads/05paper_secureplan.pdf.