Information Systems Security in a Computer Engineering Technology Program

by

Gary D. Steffen
steffen@ipfw.edu
Department of Electrical and Computer Engineering Technology
Indiana University Purdue University Fort Wayne

Abstract

In a modern Computer Engineering Technology program, a student must have sound training methods pertaining to computer and information security. The National Security Telecommunications and Information Systems Security Standard 4011 can be, partially or totally, implemented into an existing Computer Engineering Technology program. This standard, covering automated information systems (AIS), provides the minimum training standard for information systems security professionals (INFOSEC). Discussion is given pertaining to the 4011 standard which addresses the training, and challenges for incorporating such a standard into a Computer Engineering Technology program. Details will be discussed on how implementation of the standard can be distributed across multiple technical courses in the electrical, computer and programming areas.

I. Introduction

Information and computer security, once viewed by many as a threat, instigated by some young unemployed hoodlum living in their parent's basement has taken on a new face. This face of terrorism shook us on September 11th, 2001. Even though amateurs have committed most computer crimes reported to date, other attackers can be mentally deranged, overtly hostile or extremely committed to a cause [1]. A concern about these groups has led to a concentrated effort to train information professionals, as well as, general student on basic information security.

The National Security Telecommunications and Information Systems Committee (NSTISSC) established a set of standards for Information Systems Security Professionals. The NSTISSI No. 4011 standard establishes the minimum training standard for information systems security professionals in the disciplines of telecommunications and automated information systems (AIS) security [2]. The NSTISSI 4011 is the first in a series of minimum training and education standards established by the federal government. These standards can be used as guidelines for the training of Computer Engineering Technology students in the area of information security.

A deficiency in the number of trained professionals has been a growing problem. Today's savvy and novice computer user has become accustomed to words like virus, worm, spam and phishing. These are important topics to the home computer user but this simple knowledge does not meet the needs for complex information systems and networks found in industry today.

Several initiatives have been implemented to address this shortage, from educating faculty to teach information assurance to developing new information assurance (IA) programs for students [3]. In particular, the National Security Agency (NSA) has funded several programs in Information Assurance and Security under the Information Assurance Awareness, Training, and Education Partnership (IAATREP) Program. The IAATREP program was funded with the long-term goal of improving the national state of information assurance.

The short-term outcome of the IAATREP program is to provide quality education and training in Information Assurance to educators. Increasing the number of educators well versed in IA will, in turn, help to increase the number of qualified students entering the IA field. This will help increase the number of IA professionals qualified to help safeguard our nation's increasingly vulnerable information infrastructure [4]. It is through this training and documentation that information assurance can be implemented into existing computer engineering technology programs.

II. History of Information Systems Security

Communications security (COMSEC), originally for telephone communication, is defined as "measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC now includes: crypto security, transmission security, emission security, and physical security of COMSEC material" [5]. In the earliest days of wired communication, COMSEC was a concern. In those days active and passive wiretapping was easily performed with out concern of being caught. This could be done simply by picking up a phone on a multiple phone line.

As computers became developed, they were also integrated into security plans. Computer security (COMPSEC) is defined as "measures and controls that ensure confidentiality, integrity and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated" [5]. The main concerns of computer security were hackers, malicious code, users, and access. [13]

As computers began communicating over telephone lines and eventually the Internet, communications security and computer security merged into information systems security. Information systems security (INFOSEC) is defined as "protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats" [5]. This merger creating INFOSEC became the basis of the NSTISSI No. 4011 standard.

III. Information Systems Security Model

The Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), has drafted standards on many issues of information security including the 4011 standard. Included in this standard was a model of security. This model defines the areas that must be addressed in an information security plan [2].

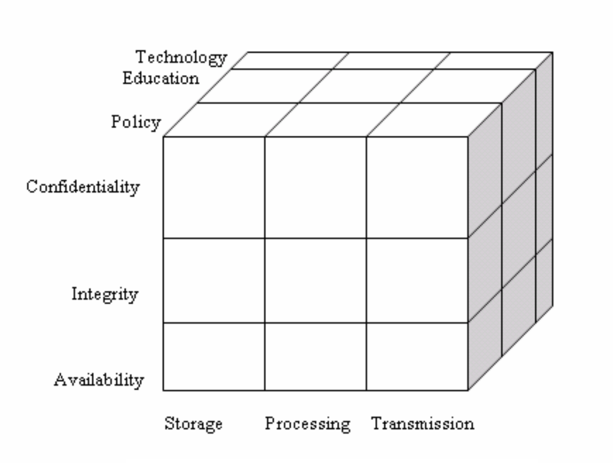

Figure 1 – Information

Imagine a three-dimensional cube (See figure 1). One axis contains the security services (confidentiality, integrity, and availability). Another axis contains the information states (storage, processing, and transmission). The last axis contains the security countermeasures (policy and practice, education, and technology). This three-dimensional cube creates twenty-seven cross sections from the intersection of the rows and columns. In order to have a valid security plan, you should address all twenty-seven cross-sections. It takes all of the individual cross-sections to make a complete plan. [13]

Upholding the three security services is a primary goal. These services are defined as:

- Confidentiality: Information is accessible only to those authorized having access.
- Integrity: Protection of the accuracy and completeness of information.
- Availability: Authorized users have access to information when required. In anything you do, you should keep the goal of preserving those three principles.

In a more recent version of the same model, two additional services have been identified [6].

- Authentication: Establish the validity of a transmission, message, or originator.
- Non-repudiation: Assurance that the sender has proof of delivery and the recipient has proof of the sender’s identity, so neither can later deny having processed the data.

The security services are used to protect information. Information can be located in:

- Storage: Information that is stationary either in electronic or physical form.
- Transmission: Information is traveling between storage locations or processing.
- Processing: Information is being handled by some intermediate process between storage and transmission.

Three methods exist to secure information: technology, education, and policy. The focus of many individuals is on technology. We install the latest security technology and then we call it secure. Technology is actually one of the smallest parts of security.   As figure 2 demonstrates, the foundation of all countermeasures is awareness, training, and education. Most compromises of security is due to lack of knowledge and training. If you have no knowledge training of security technology, how can you call it safe? Furthermore, you cannot implement technology until you have valid policy and practices of the technology. All organizations must recognize that security is not a technology, but rather a multiple part process. Without policy and practices and awareness, training, and education, your security plan is not valid.[13]

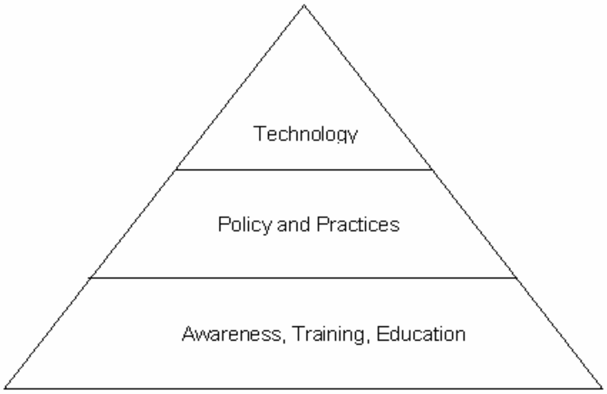

Figure 2 – Information Assurance

The information system security now also includes Information Assurance (IA). This encompasses information systems and the information itself. Information assurance is defined as “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities” as seen in figure 3 [7] [13].

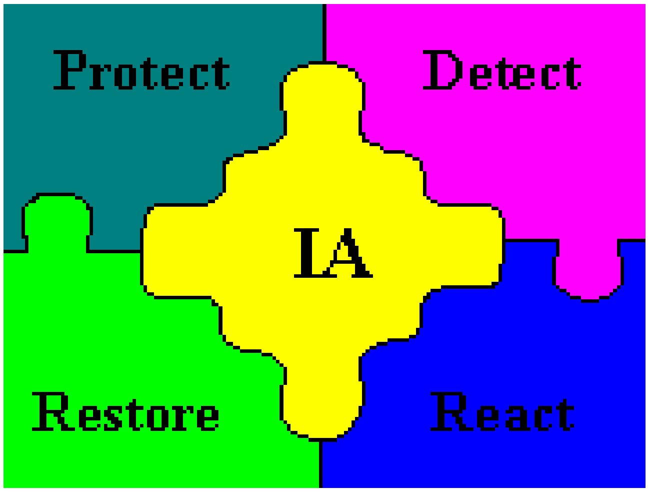

Figure 3 – Information Assurance

IV. NSTISSI No. 4011 – The Training Standard for INFOSEC

The NSTISSI No. 4011 standard establishes "the minimum training standard for INFOSEC professionals in the discipline of telecommunications and automated information systems (AIS)" [2]. It focuses on seven areas: Communications Basics, Automated Information Systems (AIS) Basics, Security Basics, NSTISS Basics, System Operating Environment, NSITSS Planning and Management, NSTISS Policies and Procedures. The standard also establishes the level at which an INFOSEC specialist should be trained. A list of behavioral outcomes for the 4011 standard can be found in appendix A.

The standards are written to provide two levels of knowledge [2]:

1. Awareness level: Creates sensitivity to the threats and vulnerabilities of national security information and recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices INFOSEC.
2. Performance level: Provides the employee with the skill or ability to design, execute, or evaluate agency INFOSEC procedures and practices. This level of understanding will ensure employees are able to apply security concepts while performing their tasks.

An additional benefit of using the NISTISSI Standard is that an institution can seek accreditation as a "Center for Academic Excellence in Information Assurance Education (CAEIAE)." The mapping of the NSTISSI No. 4011 standard is part of the requirements of the accreditation. Once certification is complete, students can receive certificates indicating they have completed the training. Furthermore with accreditation, additional grant opportunities open up to the institution [13].

V. Course Mapping for a Computer Engineering Technology Program

The Computer Engineering Technology (CPET) bachelor's degree offered at Indiana University-Purdue University Fort Wayne (IPFW) was designed to meet regional needs that include credit and non-credit training in electrical, electronics, computer applications, and computer networking. The department of Electrical and Computer Engineering Technology (ECET) furthermore seeks to advance and share technical knowledge through teaching and creative endeavors, and to work with regional industries to develop and increase technically knowledgeable human resources.

As part of this endeavor, ECET has strived to provide information assurance education and training to students and professionals using the NITISSI 4011 standard. While completing the Information Assurance Education Graduate Certificate presented by the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University [12], the author began integration of the 4011 standard into the curriculum.

The ECET department of IPFW integrates the complete NSTISSI 4011 standard into existing courses. Students pursuing a bachelor of science in CPET or the networking certificate automatically complete the entire mapping of the 4011 standard. The Networking Certificate is ideal for Non-ECET students or alumni looking for additional knowledge in networking. Even though the 4011 maps to the coursework, the department has not yet sought CAEIAE accreditation. Application for accreditation requires covering coursework for the NSTISSI No. 4011 and one additional standard.

CAEIAE intuitions receive official recognition from the U.S. government and exposure for securing the nation's information systems. Students that attend CAEIAE institutions are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program (SFS). Designation as a CAEIAE does not carry a commitment for funding from the NSA or the DHS but can be valuable when applying for grant funding.

Currently one course, CPET 364, directly targets security. The other courses include modules and topical discussion on security related issues. The following six course sequence covers the NSTISSI 4011:

> CPET 264 – Programming Language Applications
> Examination of fundamental principles and issues in embedded applications: instrumentation, data acquisition, robots, and real time systems. This class will provides an overview of the C programming environment. Introduction to C language syntax, basic data types, complex data types (pointer, array, structure, bit fields, union enum) storage classes, operators, preprocessor directives, macros, functions, flow control, and file I/O. Programming using a structured approach. Emphasis on the use of mathematical functions (routines) libraries and numerical algorithms needed in embedded applications.
>
> CPET 181 - Computer Operating Systems Basics
> Introduction to computer operating systems, organization and functions of hardware components, and system software. Emphasis on system commands, operating system interface, system utilities, shells programming, file systems and management. Introduction to concepts of graphical user interface, device drivers, memory management, processes, concurrency, security, scheduling, multitasking and multiprocessing is addressed. Laboratory experiments include Microsoft Windows, and UNIX.
>
> CPET 281-Local Area Networks and Management
> A study of issues in local area network (LAN) planning, design, installation and management is completed in this course. Topics include LAN components and protocols, topologies, and network architecture, network system hardware consideration, LAN design and network layout, wiring and installation, network operating systems, network servers, connection and servers, connections and services for clients, network system administration and management. Other topics may include LAN applications, performances tuning, disaster recovery, hybrid networking environment and integration, network monitoring tools, and network management tools. Laboratory experiences include Microsoft Windows NT and UNIX

CPET 355-Data Communications & Networking Class
A study of data communications and networking techniques, protocols, and standards is done. Topics include OSI model, TCP/IP protocols and applications, signals, encoding and modulating, transmission of data and interfaces, transmission media, multiplexing, error detection and correction, data link controls, switching techniques, local area networks, wide area networks, ISDN, DSL and other well known network services.

CPET 364-Networking Security
This course examines the analysis, design, implementation, and management issues surrounding effective network security. The business, conceptual, and technological aspects of network security for computer networks will be examined. Topics include virus protection, firewalls, authentication, encryption, wireless security, security protocols, and network security policy development and fraud protection.

CPET 384 (Wide Area Network Design)
This course explores wide area network (WAN) planning and design issues. Emphasis on WAN switching methods and technologies, protocols, and services, traffic engineering and capacity planning design and security is covered. Representative case studies will be used. Other topics may include remote access technologies, access networks, backbone networks, enterprise WAN networks, remote monitoring tools and protocol analyzer, trends in WAN design and LAN/WAN integration.

Appendix B contains a complete mapping of the six ECET course to the NSTTISI 4011 standards. This mapping ensures that a graduate of the Computer Engineering Technology at IPFW meets minimum standard for an INFOSEC professional.

VI. Challenges of Implementing Security Assurance

Mapping the NSTISSI 4011 in Computer Engineering Technology program can be quite challenging if attempted all at onetime. The structure of the standard allows for the incorporation of topics into the subject matter over a period of time. The author, in this case, was able to implement the standards in multiple courses as they were instructed.

An initial challenge encountered was lack of faculty expertise. While the author had knowledge of IA he had no real working knowledge. This was initially addressed by readings and attending workshops. In the summer of 2003, the author obtained an Information Assurance Graduate Certificate from Purdue University through a program sponsored by the NSA. It was during this time that the NSTISSI No. 4011 mapping began.

At the outset of reviewing the 4011 standard, it was found that many of the current IPFW Computer Engineering Technology classes already covered points within the standard. The Network Security course, CPET 364, in particular touched upon many of these topics. It was a matter of identifying which course would best map to a particular topic standard.

A key in the alignment process was picking the proper textbook for the courses. Particular care was taken in selecting a book for the capstone course on security, CPET 364. A number of textbooks exist that have been developed tracing the NSTISSI No. 4011 standard. Choosing a text such as this ensures compliance to the standard. Having a capstone security course, such as CPET 364, lends itself well to mapping but it isn't capable of covering the complete standard.

A number of other courses, five, needed to be altered. In several cases, modules were added to courses to cover needed IA topics. Modules were developed for the programming course to ensure secure programming techniques. Additional modules were developed in Local and Wide Area networking to cover secure system administration and security policies. Syllabuses, in each course, were altered to ensure that specific standards topics would be covered.

The certification process of NSTISSI No. 4011 does not address the quality of the presentation of the material within the courseware; it simply ensures that all of the elements of a specific standard are included [14]. Even though the committee on National Security Systems (CNSS), who certifies the courseware, does not require assessment; ECET assesses the program through their accreditation body, ABET.

Since CNSS only looks for inclusion of topics, laboratories would not be necessary but this would be impractical in a technology based program. New Laboratories have been developed and some old labs have been updated to include information assurance topics. Below is a list of new laboratories.

- Encryption Methods: DES, AES and Hash technologies are used by the student.
- Steganogrpahy: The student learns about the art of hiding information within images or text files.
- KERBROS and Key Exchange: Microsoft KERBROS and public key management is used.
- Computer Virus and Protection Methods: Standard techniques of virus and worm protection is addressed, as well as, how viruses are constructed.
- Salami Attack: The student creates a program to steal small bits of data over time.
- Firewall: Performance, installation and management of firewalls are addressed.
- IDS: Intrusion Detection Systems, commercial and non-commercial are developed.
- PGP: Secure encrypted email and computer trusts are put into practice.
- Security Policy: Students write security polices.
- Secure Programming: This affords students opportunity to identify insecure programming and the creation of secure programs.
- Authentication Methods: The use of good passwords and how authentication takes place.

The ECET department is in the early stages of development and implementation of the NSTISSI NO.4011 standard. The assessment of the standard is done using normal testing and laboratories. Preliminary results have come mostly from the CPET 364 Networking Security course. Students have shown mastery of course content through satisfactory completion of topics. Ongoing assessment overall will occur as information comes available from other courses.

Conclusion

As computers become more cost effective, as Web-based Internet devices continue to be added, and data traffic rates and congestion rise, there will be a need for well trained security specialists. These specialists can come from many different diverse backgrounds, including Computer Engineering Technology, but they all must possess a standard skill set. The NSTISSI No. 4011 is one such skill set.

Standards will continue to change. The Committee on National Security Systems (CNSS) has continued to develop other more specialized standards that university degrees may align. The knowledge of NSTISSI No. 4011 is the foundation needed before pursuing any of the additional standards. These other standards include:

- NSTISSI No. 4012 – Designated Approving Authority (DAA) [8];
- NSTISSI No. 4013 – System Administration in Information Systems Security (INFOSEC) [9];
- NSTISSI No. 4014 – Information Systems Security Officers (ISSO) [10];
- NSTISSI No. 4015 – System Certifiers [11].

The National Security Telecommunications and Information Systems Security Standard 4011 was created to produce Information Systems Security (INFOSEC) Professionals. Many Computer Engineering Technology programs are well suited to be mapped to such a standard. Once mapped, graduates will possess the needed knowledge to purse security related jobs or better secure the information in their other engineering related work.

References

1. Charles P Pfleeger. and Sharie Pfleeger, "Security in Computing", 3rd edition, Prentice Hall, 2003, p. 19
2. "NSTISSI No. 4011 National Training Standard for Information Systems Security (INFOSEC) Professionals", Washington, DC: National Security Telecommunications and Information Systems Security Committee, June 1994, http://niatec.info/pdf/4011.pdf
3. M.K. Spanninger (2001, May). "Developing security competencies through information assurance undergraduate and graduate programs", 5th National Colloquium for Information Systems Security Education, Fairfax, VA, May 2001
4. "Overview of the NSA IAATREP Program.(n.d.)", Center for Education and Research in Information Assurance and Security, Purdue University, October 1 2003, http://www.cerias.purdue.edu/education/post_secondary_education /undergrad_and_grad/faculty_development/info_assurance_education/overview_nsa.php
5. "CNSS Instruction No. 4009", National Information Assurance (IA) Glossary, Committee on National Security Systems, Washington, DC, May 2003, http://niatec.info/pdf/4009.pdf
6. W. Victor Maconachy, "A Model for Information Assurance: An Integrated Approach", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, June 2001
7. W. Victor Maconachy, "Information Systems Security Educational Needs", 3rd National INFOSEC Education Colloquium, May 1999,
8. "NSTISSI No. 4012 National Training Standard for Designated Approving Authority (DAA)", National Security Telecommunications and Information Systems Security Committee, Washington, DC, August 1997, http://niatec.info/pdf/4012.pdf
9. "NSTISSI No. 4013 National Training Standard for System Administrators in Information Systems Security (InfoSec)", National Security Telecommunications and Information Systems Security Committee, Washington, DC, August 1997 http://niatec.info/pdf/4013.pdf
10. "NSTISSI No. 4014 National Training Standard for Information Systems Security Officers (ISSO)", National Security Telecommunications and Information Systems Security Committee, Washington, DC, August 1997 http://niatec.info/pdf/4014.pdf
11. "NSTISSI No. 4015 National Training Standard for System Certifiers", National Security Telecommunications and Information Systems Security Committee, Washington, DC, June 1994, http://niatec.info/pdf/4015.pdf
12. "*Information Assurance Education Graduate Certificate Program* (n.d.)", Center for Education and Research in Information Assurance and Security, Purdue University, October 1 2003 http://www.cerias.purdue.edu/education/post_secondary_education/ undergrad_and_grad/faculty_development/info_assurance_education/
13. G.D. Steffen, M.L. Ramage and C.J. Justice, "Implementing the NSTISS 4011 Standard" Telecommunications Management System 2004, Louisville, Kentucky, April 2004
14. *"IA Courseware Evaluation Program"*, National Security Agency, Washington, DC, January 2007, http://www.nsa.gov/ia/academia/iace.cfm?MenuID=10.1.1.1

Appendix A

NSTISSI No. 4011 Behavioral Outcomes [2]

a. Communications Basics
   - Outline chronology of communications systems and development
   - Match features of transmission to descriptors (e.g., signal types, speed, production characteristics, etc.)

b. Automated Information Systems (AIS) Basics
   - Define terms in an AIS
   - Define functions performed
   - Describe interrelationship among AIS components

c. Security Basics
   - The student will list and describe the elements of AIS security.
   - The student will summarize disciplines used in protecting government automated information systems.
   - Student will give examples of determinants of critical information.

d. NSTISS Basics
   - Outline national NSTISS Policies
   - Cite examples of threats and vulnerabilities of an AIS
   - Give examples of Agency implementation of NSTISS policy, practices and procedures.

e. System Operating Environment
   - Summarize Agency AIS and telecommunications systems in operation.
   - Give examples of current Agency AIS / telecommunications systems and configurations.
   - List Agency-level contact points for AIS and telecommunications systems and maintenance
   - Cite appropriate policy and guidance.

f. NSITSS Planning and Management
   - Builds a security plan that encompasses NSTISS components in designing protection / security for an instructor-supplied description of an AIS / telecommunications system.

g. NSTISS Policies and Procedures
   - Playing the role of either a system penetrator or system protector, the student will discover points of exploitation and apply appropriate countermeasures in an instructor-supplied description of an Agency AIS/telecommunications system.

Appendix B
ECET NSTISSI 4011 Mapping [13]

NSTISSI 4011 Mappings for the Information Security Program					
	CPET 181/ ECET 264	CPET 281	CPET 355	CPET 364	CPET 384
a. COMMUNICATIONS BASICS (Awareness Level)					
(a) Historical vs Current Methodology	X			X	
(b) Capabilities and limitations of various communications systems		X	X		
b. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS					
(a) Historical vs Current Technology				X	
(b) Hardware	X			X	
(c) Software				X	
(d) Memory	X			X	
(e) Media		X			X
(f) Networks		X			X
c. SECURITY BASICS (Awareness Level)					
(a) INFOSEC Overview				X	
(b) Operations Security (OPSEC)	X	X			
(c) Information Security		X		X	
(d) INFOSEC				X	
d. NSTISS BASICS (Awareness Level)					
(a) National Policy and Guidance				X	
(b) Threats to and Vulnerabilities of Systems	X	X		X	X
(c) Legal Elements				X	
(d) Countermeasures	X	X		X	X
(e) Concepts of Risk Management				X	
(f) Concepts of System Life Cycle Management				X	
(g) Concepts of Trust		X			
(h) Modes of Operation	X				
(i) Roles of Various Organizational Personnel	X	X		X	
(j) Facets of NSTISS					
e. SYSTEM OPERATING ENVIRONMENT (Awareness Level)					
(a) AIS			X	X	
(b) Telecommunications Systems			X		
(c) Agency Specific Security Policies				X	
(d) Agency Specific AIS and Telecommunications Policies			X		
f. NSTISS PLANNING AND MANAGEMENT (Performance Level)					
(a) Security Planning	X	X		X	
(b) Risk Management		X		X	X
(c) Systems Life Cycle Management				X	
(d) Contingency Planning/Disaster Recovery		X		X	
g. NSTISS POLICIES AND PROCEDURES (Performance Level)					
(a) Physical Security Measures	X			X	
(b) Personnel Security Practices and Procedures	X	X		X	X
(c) Software Security	X	X		X	
(d) Network Security			X		X
(e) Administrative Security Procedural Controls				X	
(f) Auditing and Monitoring		X		X	
(g) Cryptosecurity				X	
(h) Key Management				X	
(i) Transmission Security			X		
(j) TEMPEST Security				X	