NSTISSI 4011 Map to JSU Courses

Completed by: Dr. Guillermo A. Francia, III

As of: 08/08/2008

	CS 201	CS 232	CS 307	CS 310	CS 450	CS 470
A. COMMUNICATIONS BASICS (Awareness Level)						
Instructional Content						
Describe vehicles of transmission					III	
Introduce the evolution of modern communications systems					I	
(1) Topical Content						
(a) Historical vs. Current Methodology					I	
(b) Capabilities and limitations of various communications systems					III	
Asynchronous vs. synchronous					III.b	
Dedicated line					III.e	
Digital vs. analog					III.b	
Line of sight					III.c	
Microwave					III.c	
Public switched network					III.e	
Radio frequency (e.g., bandwidth)					III.c	
Satellite					III.d	
B. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS (Awareness Level)						
Instructional Content						
Describe an AIS environment	I					
Provide language of an AIS	I				I	
Providing an overview of hardware, software, firmware components of an AIS to integrate into information systems security aspects/behaviors discussed later	I				I	
(1) Topical Content						
(a) Historical vs. Current Methodology	I					
(b) Hardware					I.a	
Components (e.g., I/O, CPU)	I.a				I.a	
Distributed vs. stand alone	I.f				I.a	
Micro, mini, mainframe processors	I.a				I.a	
Storage devices	I.c				I.a	
(c) Software					I.b	
Applications	I.b				I.b	
Operating system	I.b				I.b	
(d) Memory						
Random	I.c					
Sequential	I.c					
Volatile vs. nonvolatile	I.c					
(e) Media						
Magnetic remanence	I.d				III.b	
Optical remanence	I.d				III.b	
(f) Networks						
Asynchronous vs. synchronous					III.b	
File servers					I.b	
Modems					III.g	
Sharing of data					I	
Sharing of devices					I	
Switching					I.b,I.c	
Topology					I.c	
C. SECURITY BASICS (Awareness Level)						
Instructional Content						
Using the Comprehensible Model of Information Systems Security, (contained in the Annex to this instruction), introduce a comprehensive model of information systems security that addresses:						
Critical characteristics of information			I			I,II
Information states			I			I,II
Security measures			I			I,II
(1) Topical Content						
(a) INFOSEC Overview						
Critical information characteristics - availability			I			I
Information states - processing			I			II
Security countermeasures - education, training and awareness			V.d			
Critical information characteristics - integrity			I			I,V
Critical information characteristics - confidentiality			I			I,IV
Information states - storage			I			
Information states - transmission			IX			XIV
Security countermeasures - policy, procedures and practices			IV			XVI
Security countermeasures - technology			IX			IX,XI
Threats			II			XIII
Vulnerabilities			II			XIII
(b) Operations Security (OPSEC)						

			INFOSEC and OPSEC interdependency			I			
			OPSEC process			I			
			OPSEC surveys/OPSEC planning			I			
			Unclassified indicators			I			
		(c) Information Security							
			Application dependent guidance						XVI
			Policy			IV			III - VI
			Roles and responsibilities			X			XIV,XV
		(d) INFOSEC							
			Computer security - access control			IX.a			II
			Cryptography - encryption (e.g., point-to-point, network, link)			IX.g			
			Computer security - audit			IV,VII			XII
			Computer security - identification and authentication			IX			VIII
			Computer security - object reuse						XVI
			Cryptography - key management			IX			VIII
			Cryptography - strength (e.g., complexity, secrecy, characteristics of the key)			IX.g			VII.d
			Emanations security					III.h	XIII
			Physical, personnel and administrative security			X			
			Transmission security			IX		III.h	XIII,XIV
D. NSTISS BASICS (Awareness Level)									
	Instructional Content								
		Describe components of NSTISS (with examples to include: national policy, threats and vulnerabilities, countermeasures, risk management, systems lifecycle management, trust, modes of operation, roles of organizational units, facets of NSTISS).				I			
	(1) Topical Content								
		(a) National policy and guidance							
			AIS security			I, IX			I
			Communications security			IX			XIV
			Employee accountability for agency information			XI			
			Protection of information			IX			XI
		(b) Threats to and vulnerabilities of systems							
			Definition of terms (e.g., threats, vulnerabilities, risk)			II			XIII
			Major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring)			II, VII			XIII
			Threat impact areas			VII			XIII
		(c) Legal elements							
			Criminal prosecution			XI			
			Evidence collection and preservation			XIII			
			Fraud, waste and abuse			XI			
			Investigative authorities			XI			
		(d) Countermeasures							
			Assessments (e.g., surveys, inspections)			VII			
			Cover and deception			VII			
			Education, training, and awareness			V			IX
			HUMINT			V			X
			Monitoring (e.g., data, line)			IX			XII, XIV, XV
			Technical surveillance countermeasures			IX		I,V	X
		(e) Concepts of risk management							
			Consequences (e.g. corrective action, risk assessment)			IV			
			Cost/benefit analysis of controls			VIII			
			Implementation of cost-effective controls			VIII			
			Monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)			VIII			
			Threat and vulnerability assessment			VIII			XIII
		(f) Concepts of system life Cycle Management							
			Demonstration and validation (testing)		I.b	II.c			XVI.e
			Development		I.b	II.c	III.b-III.e		XVI
			Implementation		I.b	II.c	IV.a		XVI.c
			Operations and maintenance (e.g., configuration management)			II.c	IV.b		XVI.e
			Requirements definition (e.g. architecture)		I.b	VI.d	II.d		XVI.a
			Security (e.g., certification and accreditation)			VI.d			XVI
		(g) Concepts of trust							
			Assurance			I			I
			Mechanism			I			IX-XI
			Policy			I, IV			III-VI
		(h) Modes of operation							
			Compartmented/partitioned						III-VI
			Dedicated						III-VI
			Multilevel						III-VI
			System-high						III-VI
		(i) Roles of various organizational personnel							
			Audit office			X			

			COMSEC custodian			X			
			End users			X			
			Information resources management staff			X			
			INFOSEC Officer			X			
			OPSEC managers			X			
			Program or functional managers			X			
			Security office			X			
			Senior management			X			
			System manager and system staff			X			
			Telecommunications office and staff			X			
		(j) Facets of NSTISS							
			Application of cryptographic systems			IX.a			VII
			Backup of data and files						XIV, XV
			Protection against malicious logic			II.c			XVI
			Protection of areas			IX			X, XI, XIII
			Protection of data communications			IX			X, XI, XIII
			Protection of equipment			IX			X, XI, XIII
			Protection of files and data			IX			X, XI, XIII
			Protection of keying material			IX			X, XI, XIII
			Protection of magnetic storage media			IX			X, XI, XIII
			Protection of passwords			IX			X, XI, XIII
			Protection of voice communications			IX			X, XI, XIII
			Reporting security violations			V			X, XI, XIII
			Transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)						XIV, XV
E. SYSTEM OPERATING ENVIRONMENT (Awareness Level)									
	Instructional Content								
		Describe agency "control points" for purchase and maintenance of Agency AIS and telecommunications systems							
		Outline Agency specific AIS and telecommunications systems							
		Review agency AIS and telecommunications security policies							
	(1) Topical Content								
		(a) AIS							
			Firmware	I.a					
			Hardware	I.a					
			Software	I.b					
		(b) Telecommunications systems							
			Hardware	I.e					
			Software	I.e					
		(c) Agency specific security policies							
			Guidance			IV,X,XI			
			Points of contact			IV,X,XI			
			Roles and responsibilities			IV,X,XI			
		(d) Agency specific AIS and telecommunications policies							
			Points of contact			IV,X,XI			
			References			IV,X,XI			
F. NSTISS PLANNING AND MANAGEMENT (Performance Level)									
	Instructional Content								
		Discuss practical performance measures employed in designing security measures and programs							
		Introduce generic security planning guidelines/documents							
	(1) Topical Content								
		(a) Security planning							
			Directives and procedures for NSTISS policy			II			
			NSTISS program budget			II			
			NSTISS program evaluation			II			
			NSTISS training (content and audience definition)			II			
		(b) Risk management							
			Acceptance of risk (accreditation)			VII,VIII			
			Corrective actions			VII,VIII			
			Information identification			VII,VIII			
			Risk analysis and/or vulnerability assessment components			VII,VIII			
			Risk analysis results evaluation			VII,VIII			
			Roles and responsibilities of all the players in the risk analysis process			VII,VIII			
		(c) Systems lifecycle management							
			Acquisition			II.c			XVI
			Design review and systems test performance (ensure required safeguards are						

			operationally adequate)			II.c			XVI
			Determination of security specifications			II.c			XVI
			Evaluation of sensitivity of the application based upon risk analysis			II.c			XVI
			Management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into existing applications)			II.c			XVI
			Systems certification and accreditation process			II.c			XVI
		(d) Contingency planning/disaster recovery							
			Agency response procedures and continuity of operations			III			
			Contingency plan components			III			
			Determination of backup requirements			III			
			Development of plans for recovery actions after a disruptive event			III			
			Development of procedures for offsite processing			III			
			Emergency destruction procedures			III			
			Guidelines for determining critical and essential workload			III			
			Team member responsibilities in responding to an emergency situation			III			
G. NSTISS POLICIES AND PROCEDURES (Performance Level)									
	Instructional Content								
		List and describe: elements of vulnerability and threat that exist an AIS/telecommunications system with corresponding protection measures							
		List and describe: specific technological, policy, and educational solutions for NSTISS							
	(1) Topical Content								
		(a) Physical security measures							
			Alarms						XIV.e
			Building construction						XIV.e
			Cabling						XIV.e
			Communications centers						XIV.e
			Environmental controls (humidity and air conditioning)						XIV.e
			Filtered power						XIV.e
			Fire safety controls						XIV.e
			Information systems centers						XIV.e
			Physical access control systems (key cards, locks and alarms)						XIV.e
			Power controls (regulator, uninterruptible power service (UPS), and emergency power off switch)						XIV.e
			Protected distributed systems						XIV.e
			Shielding						XIV.e
			Standalone systems and peripherals						XIV.e
			Storage area controls						XIV.e
		(b) Personal security practices and procedures							
			Access authorization/verification (need to know)			X			VI, XV
			Contractors			X			VI, XV
			Employee clearances			X			VI, XV
			Position sensitivity			X			VI, XV
			Security training and awareness (initial and refresher)			X			VI, XV
			Systems maintenance personnel			X			VI, XV
		(c) Software security							
			Assurance			II.c			XVI
			Configuration management (change controls)			II.c			XVI
			Configuration management (documentation)			II.c			XVI
			Configuration management (programming standards and controls)			II.c			XVI
			Software security mechanisms to protect information (access privileges)			II.c			XVI
			Software security mechanisms to protect information (application security features)			II.c			XVI
			Software security mechanisms to protect information (audit trails and logging)			II.c			XVI
			Software security mechanisms to protect information (concept of least privilege)			II.c			XVI
			Software security mechanisms to protect information (identification and authentication)			II.c			XVI
			Software security mechanisms to protect information (internal labeling)			II.c			XVI
			Software security mechanisms to protect information (malicious logic protection)			II.c			XVI
			Software security mechanisms to protect information (need to know controls)			II.c			XVI
			Software security mechanisms to protect information (operating systems security features)			II.c			XVI
			Software security mechanisms protect information (segregation of duties)			II.c			XVI
		(d) Network security							
			Dial up versus dedicated					III.h	
			End-to-end access control					III.h	
			Privileges (class, nodes)					III.h	
			Public versus private					VI	
			Traffic analysis					I.d	
		(e) Administrative security procedural controls							
			Attribution			IV			
			Construction, changing, issuing and deleting			IV			
			Copyright protection and licensing			IV			
			Destruction of media			IV			
			Documentation, logs and journals			IV			
			Emergency destruction			IV			
			External marking of media			IV			

			Media downgraded and declassification				IV			
			Preparation of security plans				IV			
			Reporting of computer misuse or abuse				IV			
			Repudiation				IV			
			Sanitization of media				IV			
			Transportation of media				IV			
		(f) Auditing and monitoring								
			Conducting security reviews				VI			XII
			Effectiveness of security programs				VIII			XII
			Investigation of security breaches				VIII			XII
			Monitoring systems for accuracy and abnormalities				VIII			XII
			Privacy				VIII			XII
			Review of accountability controls				VIII			XII
			Review of audit trails and logs				VIII			XII
			Review of software design standards				II.c			XVI
			Verification, validation, testing, and evaluation processes				II.c			XVI
		(g) Cryptosecurity								
			Cryptovariable or key							VII
			Electronic key management system							VIII
			Encryption/decryption method, procedure, algorithm							VII
		(h) Key Management								
			Access, control and storage of COMSEC material							VIII
			Destruction procedures for COMSEC material							VIII
			Identify and inventory COMSEC material							VIII
			Key management protocols (bundling, electronic key, over-the-air rekeying)							VIII
			Report COMSEC incidents							VIII
		(i) Transmission Security								
			Burst transmission						III.h	XIV
			Convert channel control (cross talk)						III.h	XIV
			Dial back						III.h	
			Directional signals						III.h	
			Frequency hopping						III.h	XIV
			Jamming						III.h	XIV
			Line of sight						III.h	
			Line authentication						III.h	
			Low power						III.h	
			Masking						III.h	
			Optical systems						III.h	
			Protected wireline						III.h	
			Screening						III.h	
			Spread spectrum transmission						III.h	XIV
		(j) TEMPEST Security								
			Attenuation						III.h	
			Banding						III.h	
			Cabling						III.h	
			Filtered power						III.h	
			Grounding						III.h	
			Shielding						III.h	
			TEMPEST separation						III.h	
			Zone of control/zoning						III.h	XV.g