

NSTISSI 4011 mapping to AACC Courses

		CSI 113	CSI 130	CSI 165	CSI 214	CSI 258	CSI 270	CSI 265
A. COMMUNICATIONS BASICS (Awareness Level)								
	Instructional Content							
	Describe vehicles of transmission					2.2	6.3	
	Introduce the evolution of modern communications systems	1.2						
	(1) Topical Content							
	(a) Historical vs. Current Methodology	1.2						
	(b) Capabilities and limitations of various communications							
	Asynchronous vs. synchronous	3.1/3.2				2.2		
	Dedicated line	3.1/3.2				2.2		
	Digital vs. analog	3.1/3.2				2.2		
	Line of sight	3.1/3.2				2.2		
	Microwave	3.1/3.2				2.2		
	Public switched network	3.1/3.2				2.2		
	Radio frequency (e.g., bandwidth)	3.1/3.2				2.2		
	Satellite	3.1/3.2				2.2		
B. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS								
	Instructional Content							
	Describe an AIS environment	5.1/6.2						
	Provide language of an AIS	4.1						
	Providing an overview of hw, sw, fw components of an AIS to integrate into info sys security aspects/behaviors discussed later	2.0/4.0				6.0		
	(1) Topical Content							
	(a) Historical vs. Current Technology	1.2/4.6						
	(b) Hardware							
	Components (e.g., I/O, CPU)*	2.1/2.3						
	Distributed vs. stand alone	2.1-2.3						
	Micro, mini, mainframe processors	1.2						
	Storage devices	2.3/2.4						

		(c) Software							
		Applications	4.0						
		Operating system						4.1.1	
		(d) Memory							
		Random	2.1						
		Sequential	2.1						
		Volatile vs. nonvolatile	2.1/2.2						
		(e) Media							
		Magnetic remanance			2.2				11.1.1/3.2
		Optical remanance			2.2				
		(f) Networks							
		Asynchronous vs. synchronous	3.1						
		File servers	3.2						
		Modems	3.1						
		Sharing of data	3.2						
		Sharing of devices	3.2						
		Switching	3.2					1.0	
		Topology	3.2						
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						1.4	2.4.1
		Information states						1.5	
		Security measures						1.5	4.0
(1) Topical Content									
		(a) INFOSEC Overview							
		Critical information characteristics - availability						1.4	2.4(2.4.1)
		Critical information characteristics - confidentiality						1.4	2.4(2.4.1)
		Critical information characteristics - integrity						1.4	2.4(2.4.1)
		Information states - processing				13.0			
		Information states - storage				10.3			
		Information states - transmission				10.2			
		Security countermeasures - education, training and awareness						6.9	

		Security countermeasures - policy, procedures and practices				6.1			
		Security countermeasures - technology				8.0		2.8.2	
		Threats				2.2		2.8	
		Vulnerabilities				2.3			
		(b) Operations Security (OPSEC)							
		INFOSEC and OPSEC interdependency				13.1		11.0	
		OPSEC process				13.1		11.0	
		OPSEC surveys/OPSEC planning				13.2		11.0	
		Unclassified indicators				13.3		11.0	
		(c) Information Security							
		Application dependent guidance				13.4		10.0	
		Policy				6.1		2.9	
		Roles and responsibilities				11.2		2.2	
		(d) INFOSEC							
		Computer security - access control				8.0		3.0	
		Computer security - audit						3.9	17.4
		Computer security - identification and authentication			2.0			3.3	
		Computer security - object reuse			2.0			3.10.1	
		Cryptography - encryption				8.8		7.5	
		Cryptography - key management				8.8		7.10	
		Cryptography - strength (e.g., complexity, secrecy, characteristics of the key)				8.8		7.9	
		Emanations security				13.5		3.10.2	
		Physical, personnel and administrative security				9.0/11.0		11.1.1	
		Transmission security			10.2			6.0	
D. NSTISS BASICS (Awareness Level)									
	Instructional Content								
		Describe components (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.						1.0	
	(1) Topical content								
	(a) National policy and guidance								
		AIS security				6.1-6.6			
		Communications security				6.4/6.6			

		Employee accountability for agency information				11.4			
		Protection of information				1.5/6.4-6.6			
		(b) Threats to and vulnerabilities of systems							
		Definition of terms (e.g., threats, vulnerabilities, risk)				1.2			
		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)			3.0	11.0			
		Threat impact areas			3.0	11.0			
		(c) Legal elements							
		Criminal prosecution				3.1		9.9	
		Evidence collection and preservation			17.1			9.9	
		Fraud, waste and abuse				3.1		9.9	
		Investigative authorities				3.7		9.9	
		(d) Countermeasures							
		Assessments (e.g., surveys, inspections)				12.0		2.3	
		Cover and deception				11.0			
		Education, training, and awareness				6.9		2.12	
		HUMINT				13.6		1.3	
		Monitoring (e.g., data, line)			12.2/12.3			3.11/9.6	
		Technical surveillance countermeasures				12.1-12.3		4.0	
		(e) Concepts of risk management							
		Consequences (e.g. corrective action, risk)				5.3		2.0	
		Cost/benefit analysis of controls				5.3		2.4.8	
		Implementation of cost-effective controls				5.7		2.3	
		Monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)				5.7		2.3	
		Threat and vulnerability assessment				4.1-4.3		2.8	
		(f) Concepts of system life Cycle Management							
		Demonstration and validation (testing)				1.1/1.9/1.11/11.3		10.9	
		Development				1.1/1.9/1.11/11.3		10.9	
		Implementation				1.1/1.9/1.11/11.3		10.9	

			Operations and maintenance (e.g., configuration management)				1.1/1.9/1.11/11.3		10.9/11.1.1.3.1	
			Requirements definition (e.g. architecture)				1.1/1.9/1.11/11.3		10.9	
			Security (e.g., certification and accreditation)				1.1/1.9/1.11/11.3		10.9/4.9	
		(g) Concepts of trust								
			Assurance			14.1			4.2	
			Mechanism			14.1			4.2	
			Policy			14.1			4.2	
		(h) Modes of operation								
			Compartmented/partitioned				6.3/6.6/ 6.7		4.4	
			Dedicated				6.3/6.6/ 6.7		4.4	
			Multilevel				6.3/6.6/ 6.7		4.4	
			System-high				6.3/6.6/ 6.7		4.4	
		(i) Roles of various organizational personnel								
			Audit office				11.0/11.2/1.2/1.13		2.2	
			COMSEC custodian				11.0/11.2/1.2/1.13		2.2	
			End users				11.0/11.2/1.2/1.13		2.2	
			Information resources management staff				11.0/11.2/1.2/1.13		2.2	
			INFOSEC Officer				11.0/11.2/1.2/1.13		2.2	
			OPSEC managers				11.0/11.2/1.2/1.13		2.2	
			Program or functional managers				11.0/11.2/1.2/1.13		2.2	
			Security office				11.0/11.2/1.2/1.13		2.2	
			Senior management				11.0/11.2/1.2/1.13		2.2	
			System manager and system staff				11.0/11.2/1.2/1.13		2.2	

			Telecommunications office and staff				11.0/11.2/1.2/1 .13		2.2	
		(j) Facets of NSTISS								
			Application of cryptographic systems							12.0
			Backup of data and files						11.2.1	13.1
			Protection against malicious logic				3.0			
			Protection of areas				15.1			
			Protection of data communications				7.2-7.4		6.0	
			Protection of equipment					9.0		
			Protection of files and data							5.1-5.9
			Protection of keying material				14.5			
			Protection of magnetic storage media					9.0		11.1.1.3.2
			Protection of passwords					9.1		3.5
			Protection of voice communications					13.7		
			Reporting security violations				12.5			
			Transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)				10.2			
E. SYSTEM OPERATING ENVIRONMENT (Awareness Level)										
Instructional Content										
		Describe agency "control points" for purchase and maintenance of Agency AIS and telecommunications systems						13.7		11.1.1.3
		Outline Agency specific AIS and telecommunications systems						13.7/6.0		4.0
		Review agency AIS and telecommunications security policies						13.7/6.0		9.12
(1) Topical Content										
(a) AIS										
		Firmware							6.0	
		Hardware			2.0					
		Software			4.0					
(b) Telecommunications systems										
		Hardware								6.0
		Software								6.0
(c) Agency specific security policies										
		Guidance						13.8/6.1		9.12

		Points of contact				13.8		2.2	
		Roles and responsibilities				13.8		2.2	
		(d) Agency specific AIS and telecommunications policies							
		Points of contact				13.8		2.2	
		References				13.8		9.12	
F. NSTISS PLANNING AND MANAGEMENT (Performance Level)									
	Instructional content								
		Discuss practical performance measures employed in designing security measures and programs				6.4		2.3	
		Introduce generic security planning guidelines/documents				6.0		2.9	
	(1) Topical Content								
	(a) Security planning								
		Directives and procedures for NSTISS policy				1.5/13.9		2.9	
		NSTISS program budget				1.5/13.9		2.1	
		NSTISS program evaluation				1.5/13.9		2.1	
		NSTISS training (content and audience definition)				1.5/13.9		2.1	
	(b) Risk management								
		Acceptance of risk (accreditation)				4.0/5.0		2.0	
		Corrective actions				4.0/5.0		2.0	
		Information identification				4.0/5.0		2.0	
		Risk analysis and/or vulnerability assessment components				4.0/5.0		2.0	
		Risk analysis results evaluation				4.0/5.0		2.0	
		Roles and responsibilities of all the players in the risk analysis process				4.0/5.0		2.0	
	(c) Systems lifecycle management								
		Acquisition				1.11			
		Design review and systems test performance (ensure required safeguards are operationally adequate)				1.11			
		Determination of security specifications				1.11			
		Evaluation of sensitivity of the application based upon				4.0			
		Management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into				13.11		2.3/10.0	
		Systems certification and accreditation process				13.10		4.9	
	(d) Contingency planning/disaster recovery								

		Agency response procedures and continuity of operations			16.0	7.0			
		Contingency plan components			16.0	7.0			
		Determination of backup requirements			16.0	7.0			
		Development of plans for recovery actions after a			16.0	7.0			
		Development of procedures for offsite processing			16.0	7.0			
		Emergency destruction procedures			16.0	7.0			
		Guidelines for determining critical and essential			16.0	7.0			
		Team member responsibilities in responding to an emergency situation			16.0	7.0			
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				13.0/13.7		6.0	
		List and describe: specific technological, policy, and educational solutions for NSTISS				13.14		4.0/1.10/2.9	
	(1) Topical content								
		(a) Physical security measures							
		Alarms			15.1/15.2				
		Building construction			15.1				
		Cabling			15.1				
		Communications centers				7.5/7.7/7.9/9.0			
		Environmental controls (humidity and air conditioning)				9.3			
		Filtered power				9.3			
		Fire safety controls				9.2			
		Information systems centers				7.5/7.7/7.9/9.0			
		Physical access control systems (key cards, locks and alarms)				9.1			
		Power controls (regulator, uninterruptible power service (UPS), and emergency power off switch)			15.1				
		Protected distributed systems			11.1-11.5				
		Shielding				9.4			
		Standalone systems and peripherals			15.1				
		Storage area controls			15.2				

		(b) Personal security practices and procedures							
		Access authorization/verification (need to know)				6.2/11.6		3.4	
		Contractors				11.5			
		Employee clearances				11.4			
		Position sensitivity				11.4			
		Security training and awareness (initial and refresher)				6.9		2.12	
		Systems maintenance personnel				11.2			
		(c) Software security							
		Assurance				1.10/6.3/13.11			
		Configuration management (change controls)				1.10/6.3/ 12.1			
		Configuration management (documentation)				1.10/6.3/ 12.1			
		Configuration management (programming standards and controls)				1.10/6.3/ 12.1			
		Software security mechanisms to protect information (access privileges)			16.4			3.4	
		Software security mechanisms to protect information (application security features)				1.6/1.7		10.0	12.0
		Software security mechanisms to protect information (audit trails and logging)						3.9	14.5-14.7
		Software security mechanisms to protect information (concept of least privilege)			16.4			3.4	
		Software security mechanisms to protect information (identification and authentication)			2.0			3.3	
		Software security mechanisms to protect information (internal labeling)		2.0				10.0	
		Software security mechanisms to protect information (malicious logic protection)			3.0			10.10	
		Software security mechanisms to protect information (need to know controls)			2.0			3.4	
		Software security mechanisms to protect information (operating systems security features)				13.11		4.1.1	12.0
		Software security mechanisms protect information (segregation of duties)				11.6		3.4/11.1.1.1	
		(d) Network security							
		Dial up versus dedicated			13.0				
		End-to-end access control			13.0			6.0	
		Privileges (class, nodes)			13.0			6.0	

		Public versus private			9.0/13.0			6.0	
		Traffic analysis							14.7
		(e) Administrative security procedural controls							
		Attribution				13.12		3.9	
		Construction, changing, issuing and deleting						3.3.3	12.6
		Copyright protection and licensing							16.0
		Destruction of media				13.12		11.1.1.3.2	
		Documentation, logs and journals						11.1.1.3	14.4-14.7
		Emergency destruction				13.12		8.1	
		External marking of media				6.2		11.1.1.3.2	
		Media downgraded and declassification				13.12		11.1.1.3.2	
		Preparation of security plans				6.1		2.1/2.9	
		Reporting of computer misuse or abuse				13.13		9.6	
		Repudiation				8.8		7.8	
		Sanitization of media				13.12		11.1.1.3.2	
		Transportation of media				13.12		11.1.1.3.2	
		(f) Auditing and monitoring							
		Conducting security reviews					12.2	3.9	
		Effectiveness of security programs			17.2/17.4			2.8	
		Investigation of security breaches			17.0	7.4			
		Monitoring systems for accuracy and abnormalities						3.9	14.7
		Privacy					11.7/3.0		
		Review of accountability controls					12.2	3.9	
		Review of audit trails and logs						3.9.1	14.5
		Review of software design standards					1.11	10.0	
		Verification, validation, testing, and evaluation					1.11	10.10	
		(g) Cryptosecurity							
		Cryptovariable or key			14.1-14.5			7.9	
		Electronic key management system					8.8	7.10	
		Encryption/decryption method, procedure, algorithm					8.8	7.5	
		(h) Key Management							
		Access, control and storage of COMSEC material				14.5			
		Destruction procedures for COMSEC material				14.5			
		Identify and inventory COMSEC material				14.5			
		Key management protocols (bundling, electronic key, over-the-air rekeying)				14.5			
		Report COMSEC incidents				14.5			

		(j) Transmission Security							
		Burst transmission			10.2				
		Convert channel control (cross talk)			10.2				
		Dial back			10.2				
		Directional signals			10.2				
		Frequency hopping			10.2				
		Jamming			10.2				
		Line of sight			10.2				
		Line authentication			10.2				
		Low power			10.2				
		Masking			10.2				
		Optical systems			10.2				
		Protected wireline			10.2				
		Screening			10.2				
		Spread spectrum transmission			10.2				
		(j) TEMPEST Security							
		Attenuation					7.1.8	3.6.4	
		Banding					5.1	6.4	
		Cabling			13.0			6.4	
		Filtered power				9.6		5.4(5.4.1)	
		Grounding			15.0			6.4	
		Shielding				9.4		6.0	
		TEMPEST separation				9.4		3.10.2/3.10.3	
		Zone of control/zoning			15.2	6.10		3.10.5	

—

—