

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
A. COMMUNICATIONS BASICS (Awareness Level)										
Instructional Content										
	Describe vehicles of transmission						Module 2/LO.1			
	No Sub-Category									
	Introduce the evolution of modern communications systems			8.0					Week 1	
	No Sub-Category									
(1) Topical Content										
	(a) Historical vs Current Methodology			2.f						
	No Subcategory									
	(b) Capabilities and limitations of various communications systems									
	asynchronous vs synchronous			8.b - 8.c						
	dedicated line			8.f						
	digital vs analog			8.b - 8.c						
	line of sight			8.i						
	microwave			8.i						
	public switched network			8.c						
	radio frequency (e.g., bandwidth)			8.i						
	satellite			8.i						
B. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS (Awareness Level)										
Instructional Content										
	Describe an AIS environment			2.f/8.0			4.h			
	No Sub-Category									
	Provide language of an AIS			3.0			4.h			
	No Sub-Category									
	Providing an overview of hw, sw, fw components of an AIS to integrate into info sys security aspects/behaviors discussed later			3.0			4.i & m	Module 6		
	No Sub-Category									
(1) Topical Content										
	(a) Historical vs Current Technology			8.0						
	No Sub-Category									
	(b) Hardware									
	Components (e.g., I/O, CPU)*			5.0						
	Distributed vs stand alone			5.0						
	Micro, mini, mainframe processors			5.0						
	Storage devices			6.0						
	(c) Software									
	Applications			3.0						
	Operating system			7.0	1.0					

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
		(d) Memory								
		Random	5.c	2.0/5.0						
		Sequential	5.c	2.0/5.0						
		Volatile vs nonvolatile	5.c	2.0/5.0						
		(e) Media								
		Magnetic remanance *	6.a	8.0						
		Optical remanance	6.b	8.0						
		(f) Networks								
		Asynchronous vs synchronous *	8.c					Module 2		
		File servers	5.f/6.f					Module 2	Week 3	
		Modems	8.f					Module 2		
		Sharing of data	9.0					Module 2		
		Sharing of devices	8.0					Module 2		
		Switching	8.f					Module 2	Week 13	
		Topology	8.c					Module 2	Week 4	
C. SECURITY BASICS (Awareness Level)										
Instructional Content										
		Using the Comprehensible Model of Information Systems Security, (contained in the Annex) address:								
		Critical characteristics of information				2.a				
		Information states				1.0				
		Security measures				2.c				
		(1) Topical Content								
		(a) INFOSEC Overview								
		Critical information characteristics - availability				2.0	4.0			
		Critical information characteristics - confidentiality				2.0	4.0			
		Critical information characteristics - integrity				2.0	4.0			
		Information states - processing *				2.0	4.0			
		Information states - storage				2.0	4.0			
		Information states - transmission				2.0	4.0			
		Security countermeasures - education, training and awareness				2.0	8.0/10.g & n			
		Security countermeasures - policy, procedures and practices				2.0	8.0/10.g & n			
		Security countermeasures - technology				2.0	8.0/10.g & n			
		Threats				3.0/4.0	10.n			
		Vulnerabilities				3.0/4.0	10.n			
		(b) Operations Security (OPSEC)								
		INFOSEC and OPSEC interdependency				2.a/2.f	10.a			
		OPSEC process				2.f	10.a			

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
			OPSEC surveys/OPSEC planning			2.f	10.b			
			Unclassified indicators			2.f	10.c			
		(c) Information Security								
			Application dependent guidance *				10.d			
			Policy				10.h			
			Roles and responsibilities				10.h			
		(d) INFOSEC								
			computer security - access control *			2.h	4.0			
			Computer security - audit			2.k	3.0			12.0
			Computer security - identification and authentication			2.i/5.a				
			Computer security - object reuse				4.n/10.j			
			Cryptography - encryption			11.0				
			Cryptography - key management			12.0				
			Cryptography - strength (e.g., complexity, secrecy, characteristics of the key)			11.0/12.0				
			Emanations security				10.e			
			Physical, personnel and administrative security			14.0	4.0			
			Transmission security			6.g	10.g			
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.				2.0				
		no subcategory								
		(1) topical content								
		(a) national policy and guidance								
			AIS security			2.0				
			communications security			6.0				
			employee accountability for agency information			16.h	4.0			
			protection of information				4.0			
		(b) Threats to and vulnerabilities of systems								
			definition of terms (e.g., threats, vulnerabilities, risk)			2.a	4.a			
			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	10.f & g			
			Threat impact areas			3.0	9.0			

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
		(c) legal elements								
		criminal prosecution				13.d				
		evidence collection and preservation				13.d				
		fraud, waste and abuse				13.d				
		investigative authorities				13.d				
		(d) countermeasures								
		assessments (e.g., surveys, inspections)				5.0 / 6.0	8.0			
		cover and deception				5.0 / 6.0	8.0			
		education, training, and awareness				16.h	8.0			
		HUMINT					8.0 / 10.f			
		monitoring (e.g., data, line)				5.0 / 6.0	8.0			
		technical surveillance countermeasures				5.0 / 6.0	8.0			
		(e) concepts of risk management								
		consequences (e.g. corrective action, risk assessment)				16.e	2.0 / 10.n			
		cost/benefit analysis of controls					10i			
		implementation of cost-effective controls				16.0/2.0	10.i			
		monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)				2.0	10.n			
		Threat and vulnerability assessment				2.0/16.e	10.g			
		(f) concepts of system life Cycle Management								
		demonstration and validation (testing)					10.j			
		development					10.j			
		implementation					10.j			
		operations and maintenance (e.g., configuration management)					10.j			
		requirements definition (e.g. architecture)					10.j			
		security (e.g., certification and accreditation)					10.j			
		(g) concepts of trust								
		assurance *				11.0				
		mechanism				11.0				
		policy				11.0				
		(h) modes of operation								
		compartmented/partitioned				2.0/16.h				
		dedicated				2.0/16.h				
		multilevel				2.0/16.h				
		system-high				2.0/16.h				
		(i) roles of various organizational personnel								
		audit office				16.h	10.h			

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
			COMSEC custodian			16.h	10.h			
			end users			16.h	10.h			
			information resources management staff			16.h	10.h			
			INFOSEC Officer			16.h	10.h			
			OPSEC managers			16.h	10.h			
			program or functional managers			16.h	10.h			
			security office			16.h	10.h			
			senior management			16.h	10.h			
			system manager and system staff			16.h	10.h			
			telecommunications office and staff			16.h	10.h			
			(j) Facets of NSTISS							
			application of cryptographic systems			11.0/12.0				
			backup of data and files				4.f, j, & k			6.0
			protection against malicious logic			3.0	10.k			
			protection of areas			14.0	4.g			
			protection of data communications			6.0				10.0/14.0
			protection of equipment			14.0	4.g & i			
			protection of files and data				4.j & k			4.0
			protection of keying material			11.0/12.0				
			protection of magnetic storage media			14.0	4.g			
			protection of passwords			2.h/5.0/14.0				
			protection of voice communications			6.g	10g			
			reporting security violations			16.d	10.m			
			transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)			6g	8.0			
E. SYSTEM OPERATING ENVIRONMENT (Awareness Level)										
Instructional Content										
			Describe agency "control points" for purchase and maintenance of				10.g			
			No Sub-Category							
			outline Agency specific AIS and telecommunications systems				4.h / 10.g			
			No Sub-Category							
			review agency AIS and telecommunications security policies				4.h / 10.g			
			No Sub-Category							
(1) Topical Content										
			(a) AIS							
			firmware *					Module 6		
			hardware	5.0						

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
		software		3.0						
		(b) telecommunications systems								
		hardware							Week 3&5	
		software							Week 6&7	
		(c) Agency specific security policies								
		guidance					10.h			
		points of contact					10.h			
		roles and responsibilities					10.h			
		(d) agencies specific AIS and telecommunications policies								
		points of contact *					10.h			
		references					10.h			
F. NSTISS PLANNING AND MANAGEMENT (Performance Level)										
		instructional content								
		discuss practical performance measures employed in designing security measures and programs					2.0 / 10.h			
		No Sub-Category								
		introduce generic security planning guidelines/documents					4.0 / 10.h			
		No Sub-Category								
		(1) Topical Content								
		(a) security planning								
		directives and procedures for NSTISS policy					10.i & n			
		NSTISS program budget					10.i & n			
		NSTISS program valuation					10.i & n			
		NSTISS training (content and audience definition)					10.i & n			
		(b.) risk management								
		acceptance of risk (accreditation)				16.e	10.n			
		corrective actions				16.e	10.n			
		information identification				16.e	10.n			
		risk analysis and/or vulnerability assessment components				16.e	10.n			
		risk analysis results evaluation				16.e	10.n			
		roles and responsibilities of all the players in the risk analysis process				16.e	10.n			
		(c.) systems lifecycle management								
		acquisition					4.m & n			
		design review and systems test performance (ensure required safeguards are operationally adequate)					4.m & n			
		determination of security specifications					4.m & n			

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
			evaluation of sensitivity of the application based upon risk analysis				4.n & 10.d			
			management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications)				4.n			
			systems certification and accreditation process				10.j			
			(d) contingency planning/disaster recovery							
			agency response procedures and continuity of operations *			16.0	4.e & f			
			contingency plan components			16.0	4.e & f			
			determination of backup requirements			16.0	4.e & f			
			development of plans for recovery actions after a disruptive event			16.0	4.e & f			
			development of procedures for offsite processing			16.0	4.e & f			
			emergency destruction procedures			16.0	4.e & f			
			guidelines for determining critical and essential workload			16.0	4.e & f			
			team member responsibilities in responding to an emergency situation			16.0	4.e & f			
G. NSTISS policies and procedures (Performance Level)										
			instructional content							
			list and describe: elements of vulnerability and threat that exist an			10.0	10.g			
			No Sub-Category							
			List and describe: specific technological, policy, and educational				10.i			
			No Sub-Category							
			(1) topical content							
			(a) physical security measures							
			alarms *			14.0	4.g			
			building construction			14.0	4.g			
			cabling			14.0	4.g			
			communications centers			14.0	4.g			
			environmental controls (humidity and air conditioning)			14.0	4.c			
			filtered power			14.0	4.d			
			fire safety controls			14.0	4.g			
			information systems centers			14.0	4.g			
			physical access control systems (key cards, locks and alarms)			14.0	4.g			

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
			power controls (regulator, uninterruptible power service (UPS), and emergency power off switch			14.0	4.d & g			
			protected distributed systems			14.0	4.g & l			
			shielding			14.0	4.d & g			
			standalone systems and peripherals			14.0	4.g & h			
			storage area controls			14.0	4.g			
		(b) personal security practices and procedures								
			access authorization/verification (need to know)			5.a / 16.h	10.a			
			contractors			16.h	10.a			
			employee clearances			16.h	10.a			
			position sensitivity			16.h	10.a			
			security training and awareness (initial and refresher)			16.h	10.a			
			systems maintenance personnel			16.h	10.a			
		(c) software security								
			assurance *				4.m & 10.k			
			configuration management (change controls)			16.f	4.m & 10.k			
			configuration management (documentation)			16.f	4.m & 10.j			
			configuration management (programming standards and controls)				4.m & 10.j & k			
			software security mechanisms to protect information (access privileges)			5.0	4.m & 10.k			
			software security mechanisms to protect information (application security's features)				4.m & 10.k			14.0
			software security mechanisms to protect information (audit trails and logging)				3.0			13.0
			software security mechanisms to protect information (concept of least privilege)			2.h/5.0				
			software security mechanisms to protect information (identification and authentication)			2.h/5.0				
			software security mechanisms to protect information (internal labeling)		8.0/9.0		4.m & 10.k			
			software security mechanisms to protect information (malicious logic protection)			3.0	4.m & 10.k			
			software security mechanisms to protect information (need to know controls)			2.h	4.m & 10.k			
			software security mechanisms to protect information (operating systems security features)				4.m & 10.a & k			14.0
			software security mechanisms protect information (segregation of duties)			2.h/16.h	4.m & 10.k			
		(d) network security								
			dial up versus dedicated *			6.0/8.0/9.0	10.g			

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
			end-to-end access control			6.0/8.0/9.0	10.g			
			privileges (class, nodes)			6.0/8.0/9.0	10.g			
			public versus private			6.0/8.0/9.0	10.g			
			traffic analysis							13.0
		(e)	administrative security procedural controls							
			attribution *				10.i			
			construction, changing, issuing and deleting passwords			5.a				14.0
			copyright protection and licensing							15.0
			destruction of media				10.i	reading - NIST 800-12 Ch 14		
			documentation, logs and journals							12.0
			emergency destruction				10.i			
			external marking of media				10.i			
			media downgraded and declassification				10.i			
			preparation of security plans			16.b	10.h			
			reporting of computer misuse or abuse			16.d	10.m			
			repudiation			11.0/15.0/16.h				
			sanitization of media				10.i	reading - NIST 800-12 Ch 14		
			transportation of media				10.i	reading - NIST 800-12 Ch 14		
		(f)	auditing and monitoring							
			conducting security reviews *			2.k	3.0			
			effectiveness of security programs			2.k	3.0			
			investigation of security breaches			2.k	3.0			
			monitoring systems for accuracy and abnormalities							13.0
			privacy			2.k	3.0			
			review of accountability controls			2.k	3.0			
			review of audit trails and logs							12.0
			review of software design standards			2.k	3.0 / 4.m			
			verification, validation, testing, and evaluation processes			2.k	3.0 / 4.m			
		(g)	Cryptosecurity							
			cryptovariable or key *			11.0 / 12.0				
			electronic key management system			11.0 / 12.0				
			encryption/decryption method, procedure, algorithm			11.0 / 12.0				
		(h)	Key Management							
			access, control and storage of COMSEC material			11.0 / 12.0				
			destruction procedures for COMSEC material			11.0 / 12.0				
			identify and inventory COMSEC material			11.0 / 12.0				
			key management protocols (bundling, electronic key, over-the-air rekeying)			11.0 / 12.0				
			report COMSEC incidents			11.0 / 12.0				

NSTISSI 4011 MAPPING - PGCC				CIS101	CIS170	CIS162	CIS269	ENT197	CIS140	CIS231
		(i) Transmission Security								
		burst transmission			6.g	10.g				
		covert channel control (cross talk)			6.g	10.g				
		dial back			6.g	10.g				
		directional signals			6.g	10.g				
		frequency hopping			6.g	10.g				
		jamming			6.g	10.g				
		line of sight			6.g	10.g				
		line authentication			6.g	10.g				
		low power			6.g	10.g				
		masking			6.g	10.g				
		optical systems			6.g	10.g				
		protected wireline			6.g	10.g				
		screening			6.g	10.g				
		spread spectrum transmission			6.g	10.g				
		(j) TEMPEST Security								
		attenuation *						Module 5		
		banding						Module 5		
		cabling			10.0					
		filtered power			14.d	4.d				
		grounding			14.0	4.d				
		shielding			14.c	4.d				
		TEMPEST separation			14.c	10.b				
		zone of control/zoning			14.b / 14.d	10.b				