

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>						
Completed by: <i>Dr. John W. Collins, Jr.</i>				<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
As of:	11/29/2006					
<b>A. COMMUNICATIONS BASICS (Awareness Level)</b>						
	<b>Instructional Content</b>					
		Describe vehicles of transmission		<b>8.1</b>		
		Introduce the evolution of modern communications systems		<b>8.2</b>		
	<b>(1) Topical Content</b>					
		(a) Historical vs. Current Methodology		<b>1</b>		
		(b) Capabilities and limitations of various communications				
		Asynchronous vs. synchronous		<b>2.1</b>		
		Dedicated line		<b>2.2</b>		
		Digital vs. analog		<b>2.3</b>		
		Line of sight		<b>2.4</b>		
		Microwave		<b>3.1</b>		
		Public switched network		<b>3.2</b>		
		Radio frequency (e.g., bandwidth)		<b>3.3</b>		
		Satellite		<b>3.4</b>		
<b>B. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS (Awareness Level)</b>						
	<b>Instructional Content</b>					
		Describe an AIS environment		<b>8.3</b>		
		Provide language of an AIS		<b>8.4</b>		
		Providing an overview of hardware, software, firmware components of an AIS to integrate into information systems security aspects/behaviors discussed later		<b>8.5</b>		
	<b>(1) Topical Content</b>					
		(a) Historical vs. Current Technology		<b>4</b>		
		(b) Hardware				
		Components (e.g., I/O, CPU)*		<b>5.1</b>		
		Distributed vs. stand alone		<b>5.2</b>		
		Micro, mini, mainframe processors		<b>5.3</b>		
		Storage devices		<b>5.4</b>		
		(c) Software				
		Applications		<b>6.1</b>		
		Operating system		<b>6.2</b>		
		(d) Memory				
		Random		<b>6.3</b>		
		Sequential		<b>6.4</b>		
		Volatile vs. nonvolatile		<b>6.5</b>		
		(e) Media				

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>						
Completed by: <i>Dr. John W. Collins, Jr.</i>				<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
As of:	11/29/2006					
		Magnetic remanence	7.1			
		Optical remanence	7.2			
		(f) Networks				
		Asynchronous vs. synchronous	7.3			
		File servers	7.4			
		Modems	7.5			
		Sharing of data	7.6			
		Sharing of devices	7.7			
		Switching	7.8			
		Topology	7.9			
<b>C. SECURITY BASICS (Awareness Level)</b>						
<b>Instructional Content</b>						
		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	15.4			
		Information states		8.1		
		Security measures		8.2		
<b>(1) Topical Content</b>						
		(a) INFOSEC Overview				
		Critical information characteristics - availability	13.1			
		Critical information characteristics - confidentiality	13.2			
		Critical information characteristics - integrity	13.3			
		Information states - processing	14.1			
		Information states - storage	14.2			
		Information states - transmission	14.3			
		Security countermeasures - education, training and awareness	14.4			
		Security countermeasures - policy, procedures and practices	14.5			
		Security countermeasures - technology	14.6			
		Threats	14.7			
		Vulnerabilities	14.8			
		(b) Operations Security (OPSEC)				
		INFOSEC and OPSEC interdependency		1.1		
		OPSEC process		1.2		
		OPSEC surveys/OPSEC planning		1.3		

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>						
Completed by: <i>Dr. John W. Collins, Jr.</i>				<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
As of:	11/29/2006					
		Unclassified indicators			<b>1.4</b>	
		(c) Information Security				
		Application dependent guidance			<b>2.1</b>	
		Policy			<b>2.2</b>	
		Roles and responsibilities			<b>2.3</b>	
		(d) INFOSEC				
		Computer security - access control			<b>3.1</b>	
		Computer security - audit			<b>3.2</b>	
		Computer security - identification and authentication			<b>3.3</b>	
		Computer security - object reuse			<b>3.4</b>	
		Cryptography - encryption			<b>4.1</b>	
		Cryptography - key management			<b>4.2</b>	
		Cryptography - strength (e.g., complexity, secrecy, characteristics of the key)			<b>4.3</b>	
		Emanations security			<b>5.1</b>	
		Physical, personnel and administrative security			<b>5.2</b>	
		Transmission security			<b>5.3</b>	
<b>D. NSTISS BASICS (Awareness Level)</b>						
	<b>Instructional Content</b>					
		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).			<b>8.3 &amp; 15</b>	
	<b>(1) Topical content</b>					
		(a) National policy and guidance				
		AIS security			<b>6.1</b>	
		Communications security			<b>6.2</b>	
		Employee accountability for agency information			<b>6.3</b>	
		Protection of information			<b>6.4</b>	
		(b) Threats to and vulnerabilities of systems				
		Definition of terms (e.g., threats, vulnerabilities, risk)			<b>7.1</b>	
		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)			<b>7.2</b>	
		Threat impact areas			<b>7.3</b>	
		(c) Legal elements				

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>					
Completed by: <i>Dr. John W. Collins, Jr.</i>					
As of:	11/29/2006		<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
		Criminal prosecution		<b>9.1</b>	
		Evidence collection and preservation		<b>9.2</b>	
		Fraud, waste and abuse		<b>9.3</b>	
		Investigative authorities		<b>9.4</b>	
		(d) Countermeasures			
		Assessments (e.g., surveys, inspections)		<b>10.1</b>	
		Cover and deception		<b>10.2</b>	
		Education, training, and awareness		<b>10.3</b>	
		HUMINT		<b>10.4</b>	
		Monitoring (e.g., data, line)		<b>10.5</b>	
		Technical surveillance countermeasures		<b>10.6</b>	
		(e) Concepts of risk management			
		Consequences (e.g. corrective action, risk		<b>10.7</b>	
		Cost/benefit analysis of controls		<b>10.8</b>	
		Implementation of cost-effective controls		<b>10.9</b>	
		Monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)		<b>10.10</b>	
		Threat and vulnerability assessment		<b>10.11</b>	
		(f) Concepts of system life Cycle Management			
		Demonstration and validation (testing)		<b>11.1</b>	
		Development		<b>11.2</b>	
		Implementation		<b>11.3</b>	
		Operations and maintenance (e.g., configuration management)		<b>11.4</b>	
		Requirements definition (e.g. architecture)		<b>11.5</b>	
		Security (e.g., certification and accreditation)		<b>11.6</b>	
		(g) Concepts of trust			
		Assurance		<b>12.1</b>	
		Mechanism		<b>12.2</b>	
		Policy		<b>12.3</b>	
		(h) Modes of operation			
		Compartmented/partitioned		<b>12.4</b>	
		Dedicated		<b>12.5</b>	
		Multilevel		<b>12.6</b>	
		System-high		<b>12.7</b>	
		(i) Roles of various organizational personnel			
		Audit office		<b>13.1</b>	
		COMSEC custodian		<b>13.2</b>	

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>					
Completed by: <i>Dr. John W. Collins, Jr.</i>					
As of:	11/29/2006		<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
		End users		<b>13.3</b>	
		Information resources management staff		<b>13.4</b>	
		INFOSEC Officer		<b>13.5</b>	
		OPSEC managers		<b>13.6</b>	
		Program or functional managers		<b>13.7</b>	
		Security office		<b>13.8</b>	
		Senior management		<b>13.9</b>	
		System manager and system staff		<b>13.10</b>	
		Telecommunications office and staff		<b>13.11</b>	
		(j) Facets of NSTISS			
		Application of cryptographic systems		<b>14.1</b>	
		Backup of data and files		<b>14.2</b>	
		Protection against malicious logic		<b>14.3</b>	
		Protection of areas		<b>14.4</b>	
		Protection of data communications		<b>14.5</b>	
		Protection of equipment		<b>14.6</b>	
		Protection of files and data		<b>14.7</b>	
		Protection of keying material		<b>14.8</b>	
		Protection of magnetic storage media		<b>14.9</b>	
		Protection of passwords		<b>14.10</b>	
		Protection of voice communications		<b>14.11</b>	
		Reporting security violations		<b>14.12</b>	
		Transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)		<b>14.13</b>	
<b>E. SYSTEM OPERATING ENVIRONMENT (Awareness Level)</b>					
	<b>Instructional Content</b>				
		Describe agency \"control points\" for purchase and maintenance of Agency AIS and telecommunications systems		<b>15.1</b>	
		Outline Agency specific AIS and telecommunications systems		<b>15.2</b>	
		Review agency AIS and telecommunications security policies		<b>15.3</b>	
	<b>(1) Topical Content</b>				
	(a) AIS				
		Firmware		<b>9.1</b>	
		Hardware		<b>9.2</b>	
		Software		<b>9.3</b>	
	(b) Telecommunications systems				

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>						
Completed by: <i>Dr. John W. Collins, Jr.</i>				<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
As of:	11/29/2006					
		Hardware		<b>10.1</b>		
		Software		<b>10.2</b>		
		(c) Agency specific security policies				
		Guidance		<b>11.1</b>		
		Points of contact		<b>11.2</b>		
		Roles and responsibilities		<b>11.3</b>		
		(d) Agency specific AIS and telecommunications policies				
		Points of contact		<b>12.1</b>		
		References		<b>12.2</b>		
<b>F. NSTISS PLANNING AND MANAGEMENT (Performance Level)</b>						
	<b>Instructional content</b>					
		Discuss practical performance measures employed in designing security measures and				<b>8.1</b>
		Introduce generic security planning guidelines/documents				<b>8.2</b>
	<b>(1) Topical Content</b>					
		(a) Security planning				
		Directives and procedures for NSTISS policy				<b>1.1</b>
		NSTISS program budget				<b>1.2</b>
		NSTISS program evaluation				<b>1.3</b>
		NSTISS training (content and audience definition)				<b>1.4</b>
		(b) Risk management				
		Acceptance of risk (accreditation)				<b>2.1</b>
		Corrective actions				<b>2.2</b>
		Information identification				<b>2.3</b>
		Risk analysis and/or vulnerability assessment components				<b>2.4</b>
		Risk analysis results evaluation				<b>2.5</b>
		Roles and responsibilities of all the players in the risk analysis process				<b>2.6</b>
		(c) Systems lifecycle management				
		Acquisition				<b>3.1</b>
		Design review and systems test performance (ensure required safeguards are operationally adequate)				<b>3.2</b>
		Determination of security specifications				<b>3.3</b>
		Evaluation of sensitivity of the application based upon risk analysis				<b>3.4</b>
		Management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into existing applications)				<b>3.5</b>
		Systems certification and accreditation process				<b>3.6</b>

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>					
Completed by: <i>Dr. John W. Collins, Jr.</i>			<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
As of:	11/29/2006				
	(d) Contingency planning/disaster recovery				
	Agency response procedures and continuity of operations				<b>4.1</b>
	Contingency plan components				<b>4.2</b>
	Determination of backup requirements				<b>4.3</b>
	Development of plans for recovery actions after a				<b>4.4</b>
	Development of procedures for offsite processing				<b>4.5</b>
	Emergency destruction procedures				<b>4.6</b>
	Guidelines for determining critical and essential				<b>4.7</b>
	Team member responsibilities in responding to an emergency situation				<b>4.8</b>
					<b>4.9</b>
<b>G. NSTISS POLICIES AND PROCEDURES (Performance Level)</b>					
<b>Instructional content</b>					
	List and describe: elements of vulnerability and threat that exist an AIS/telecommunications system with corresponding protection measures				<b>15.1</b>
	List and describe: specific technological, policy, and educational solutions for NSTISS				<b>15.2</b>
<b>(1) Topical content</b>					
	(a) Physical security measures				
	Alarms				<b>5.1</b>
	Building construction				<b>5.2</b>
	Cabling				<b>5.3</b>
	Communications centers				<b>5.4</b>
	Environmental controls (humidity and air conditioning)				<b>5.5</b>
	Filtered power				<b>5.6</b>
	Fire safety controls				<b>5.7</b>
	Information systems centers				<b>5.8</b>
	Physical access control systems (key cards, locks and alarms)				<b>5.9</b>
	Power controls (regulator, uninterruptible power service (UPS), and emergency power off switch)				<b>5.10</b>
	Protected distributed systems				<b>5.11</b>
	Shielding				<b>5.12</b>
	Standalone systems and peripherals				<b>5.13</b>
	Storage area controls				<b>5.14</b>
	(b) Personal security practices and procedures				
	Access authorization/verification (need to know)				<b>6.1</b>

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>						
Completed by: <i>Dr. John W. Collins, Jr.</i>				<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
As of:	11/29/2006					
		Contractors				<b>6.2</b>
		Employee clearances				<b>6.3</b>
		Position sensitivity				<b>6.4</b>
		Security training and awareness (initial and refresher)				<b>6.5</b>
		Systems maintenance personnel				<b>6.6</b>
		(c) Software security				
		Assurance				<b>7.1</b>
		Configuration management (change controls)				<b>7.2</b>
		Configuration management (documentation )				<b>7.3</b>
		Configuration management (programming standards and controls)				<b>7.4</b>
		Software security mechanisms to protect information (access privileges)				<b>7.5</b>
		Software security mechanisms to protect information (application security features)				<b>7.6</b>
		Software security mechanisms to protect information (audit trails and logging)				<b>7.7</b>
		Software security mechanisms to protect information (concept of least privilege)				<b>7.8</b>
		Software security mechanisms to protect information (identification and authentication)				<b>7.9</b>
		Software security mechanisms to protect information (internal labeling)				<b>7.10</b>
		Software security mechanisms to protect information (malicious logic protection)				<b>7.11</b>
		Software security mechanisms to protect information (need to know controls)				<b>7.12</b>
		Software security mechanisms to protect information (operating systems security features)				<b>7.13</b>
		Software security mechanisms protect information (segregation of duties)				<b>7.14</b>
		(d) Network security				
		Dial up versus dedicated				<b>9.1</b>
		End-to-end access control				<b>9.2</b>
		Privileges (class, nodes)				<b>9.3</b>
		Public versus private				<b>9.4</b>
		Traffic analysis				<b>9.5</b>
		(e) Administrative security procedural controls				
		Attribution				<b>10.1</b>

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>					
Completed by: <i>Dr. John W. Collins, Jr.</i>					
As of:	11/29/2006		<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
		Construction, changing, issuing and deleting			<b>10.2</b>
		Copyright protection and licensing			<b>10.3</b>
		Destruction of media			<b>10.4</b>
		Documentation, logs and journals			<b>10.5</b>
		Emergency destruction			<b>10.6</b>
		External marking of media			<b>10.7</b>
		Media downgraded and declassification			<b>10.8</b>
		Preparation of security plans			<b>10.9</b>
		Reporting of computer misuse or abuse			<b>10.10</b>
		Repudiation			<b>10.11</b>
		Sanitization of media			<b>10.12</b>
		Transportation of media			<b>10.13</b>
		(f) Auditing and monitoring			
		Conducting security reviews			<b>11.1</b>
		Effectiveness of security programs			<b>11.2</b>
		Investigation of security breaches			<b>11.3</b>
		Monitoring systems for accuracy and abnormalities			<b>11.4</b>
		Privacy			<b>11.5</b>
		Review of accountability controls			<b>11.6</b>
		Review of audit trails and logs			<b>11.7</b>
		Review of software design standards			<b>11.8</b>
		Verification, validation, testing, and evaluation			<b>11.9</b>
		(g) Cryptosecurity			
		Cryptovariable or key			<b>12.1</b>
		Electronic key management system			<b>12.2</b>
		Encryption/decryption method, procedure, algorithm			<b>12.3</b>
		(h) Key Management			
		Access, control and storage of COMSEC material			<b>12.4</b>
		Destruction procedures for COMSEC material			<b>12.5</b>
		Identify and inventory COMSEC material			<b>12.6</b>
		Key management protocols (bundling, electronic key, over-the-air rekeying)			<b>12.7</b>
		Report COMSEC incidents			<b>12.8</b>
		(i) Transmission Security			
		Burst transmission			<b>13.1</b>
		Convert channel control (cross talk)			<b>13.2</b>
		Dial back			<b>13.3</b>
		Directional signals			<b>13.4</b>

<b>NSTISSI 4011 Curriculum Map to NJCU Courses</b>						
<b>Completed by: Dr. John W. Collins, Jr.</b>				<b>SECU 222</b>	<b>SECU 322</b>	<b>SECU 422</b>
<b>As of:</b>	11/29/2006					
		Frequency hopping				<b>13.5</b>
		Jamming				<b>13.6</b>
		Line of sight				<b>13.7</b>
		Line authentication				<b>13.8</b>
		Low power				<b>13.9</b>
		Masking				<b>13.10</b>
		Optical systems				<b>13.11</b>
		Protected wireline				<b>13.12</b>
		Screening				<b>13.13</b>
		Spread spectrum transmission				<b>13.14</b>
		(j) TEMPEST Security				
		Attenuation				<b>14.1</b>
		Banding				<b>14.2</b>
		Cabling				<b>14.3</b>
		Filtered power				<b>14.4</b>
		Grounding				<b>14.5</b>
		Shielding				<b>14.6</b>
		TEMPEST separation				<b>14.7</b>
		Zone of control/zoning				<b>14.8</b>