	CIS 444: Computer Networking	CIS 521: Introduction to Information Assurance	CIS 522: Computer Forensics and Incidence Response	CIS 523: Disaster Recovery and Business Continuity	CIS 524: Information Assurance Risk Assessment
4011 Points (this might change soon)					
A. Communications Basics (Awareness Level)					
Instructional Content					
Describe vehicles of transmission	X				
Introduce the evolution of modern communication systems	X				
(1)Topical Content					
(a) Historical vs Current Methodology	X				
(b) Capabilities and limitations of various communications systems					
asynchronous vs synchronous	X				
dedicated line	X				
digital vs analog	X				
line of sight	X				
microwave	X				
public switched network	X				
radio frequency	X				
satellite	X				
B. Automated Information Systems (AIS) Basics					
Instructional Content					
Describe an AIS environment	X				
Provide language of an AIS	X				
Providing an overview of hardware, software, firmware, components of AIS to integrate into information systems security aspects/behaviors discussed later	X				
(1) Topical Content					
(a) Historical vs Current Technology	X				
(b) Hardware					
components (e.g., input, output, central processing unit (CPU))	X		X		
distributed vs stand-alone	X		X		

micro, mini, mainframe processors	X		X		
storage devices	X		X		
(c) Software					
applications	X				
operating system	X		X		
(d) Memory					
random	X		X		
sequential	X		X		
volatile vs nonvolatile	X		X		
(e) Media					
magnetic remanence	X		X		
optical remanence	X		X		
(f) Networks					
asynchronous vs synchronous	X				
file servers	X				
modems	X				
sharing of data	X				
sharing of devices	X				
switching	X				
topology	X				
C. Security Basics (Awareness Level)					
Instructional Content					
Using the Comprehensive Model of Information Systems Security (contained in the Annex to this instruction), introduce a comprehensive model of information systems security that addresses:		X			
critical characteristics of information		X			X
information states		X			X
security measures		X			X
(1) Topical Content					
(a) INFOSEC Overview					
critical information characteristics - availability		X			X
critical information characteristics - confidentiality		X			X
critical information characteristics - integrity		X			X
information states - processing		X			X
information states - storage		X			X

information states - transmission		X			X
security countermeasures - education, training and awareness		X			X
security countermeasures - Technology		X			X
security countermeasures - policy, procedures, and practices		X			X
threats		X			X
vulnerabilities		X			X
(b) Operations Security (OPSEC)					
INFOSEC and OPSEC interdependency		X			
OPSEC process		X			
OPSEC surveys/OPSEC planning		X			
unclassified indicators		X			
(c) Information Security					
application dependent guidance		X			
policy		X			
roles and responsibilities		X			
(d) INFOSEC					
computer security - access control		X			X
computer security - audit					X
computer security - authentication and identification		X			
computer security - object reuse		X			
cryptography - encryption (e.g., point-to-point, network, link)		X			X
cryptography - key management (to include electronic key)		X			
cryptography - strength (e.g., complexity, secrecy, characteristics of the key)		X			
emanations security		X			
physical, personnel and administrative security		X			

transmission security		X			
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		X			X
(1) Topical Content					
(a) National Policy and Guidance					
AIS Security		X			X
communications security		X			X
employee accountability for agency information		X			X
protection of information		X			X
(b) Threats to Vulnerabilities of Systems					
definition of terms (e.g., threats, vulnerabilities, risk)		X	X		X
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)			X		
threat impact areas			X		
(c) Legal Elements					
criminal prosecution			X		
evidence collection and preservation			X		
fraud, waste and abuse			X		
investigative authorities			X		
(d) Countermeasures					
assessments (e.g., surveys, inspections)			X		X
cover and deception			X		X
education, training and awareness			X		X
HUMINT			X		X
monitoring (e.g., data, line		X	X		X

technical surveillance countermeasures		X	X		X
(e) Concepts of Risk Management					
consequences (e.g., corrective action, risk assessment					X
cost/benefit analysis of controls					X
implementation of cost-effective controls					X
monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)					X
threat and vulnerability assessment					X
(f) Concepts of System Life Cycle					
demonstration and validation (testing)		X			
development		X			
implementation		X			
operations and maintenance (e.g., configuration management)		X			
requirements definition (e.g., architecture)		X			
security (e.g., certification and accreditation)		X			
(g) Concepts of Trust					
assurance		X			X
mechanism		X			X
policy		X			X
(h) Modes of Operation					
compartmented/partitioned		X			
dedicated		X			
multilevel		X			
system-high		X			
(I) Roles of Various Organizational Personnel					
audit office		X			X
COMSEC custodian		X			X
end users		X			X
information resources management staff		X			X
INFOSEC officer		X			X
OPSEC managers		X			X

program or functional managers		X			X
security office		X			X
senior management		X			X
system manager and system staff		X			X
telecommunications office and staff		X			X
(j) Facets of NSTISS					
application of cryptographic systems		X			
backup of data and files		X			X
protection against malicious logic		X			X
protection of areas		X			
protection of data communications		X			X
protection of equipment		X			
protection of files and data		X			
protection of keying material		X			
protection of magnetic storage media		X			
protection of passwords		X			
protection of voice communications		X			
reporting of security violations		X			
transmission security countermeasures (e.g., callsigns, frequency, and pattern forwarning protection)		X			
E. System Operating Environment (Awareness					
Instructional Content					
Describe Agency "control points" for purchase and maintenance of Agency AIS and telecommunications systems		X			
Outline Agency specific AIS and telecommunications systems		X			
Review Agency AIS and telecommunications security policies		X			X
(1) Topical Content					
(a) AIS					
firmware		X			
hardware		X			
software		X			

(b) Telecommunications Systems					
hardware		X			
software		X			
(c) Agency Specific Security Policies					
guidance		X			
points of contact		X			
roles and responsibilities		X			
(d) Agency Specific AIS and					
points of contact		X			
references		X			
F. NSTISS Planning and Management (Performance					
Instructional Content					
Discuss practical performance measures					X
Introduce generic security planning		X		X	
(1) Topical Content					
(a) Security Planning					
directives and procedures for NSTISS policy	X				
NSTISS program budget	X				
NSTISS program evaluation	X				
NSTISS training (content and audience definition	X				
(b) Risk Management					
acceptance of risk (accreditation)					X
corrective actions					X
information identification					X
risk analysis and/or vulnerability assessment components					X
risk analysis results evaluation					X
roles and responsibilities of all the players in the risk analysis process					X
(c) Systems Life Cycle Management					
acquisition		X			
design review and systems test performance (ensure required safeguards are operationally adequate)		X			
determination of security specifications		X			

evaluation of sensitivity of the application based upon risk analysis		X			
management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications)		X			
systems certification and accreditation process		X			
(d) Contingency Planning/Disaster Recovery					
agency response procedures and continuity of operations				X	
contingency plan components				X	
determination of backup requirements				X	
development of plans for recovery actions after a disruptive event				X	
development of precedures for off-site processing				X	
emergency destruction procedures				X	
guidelines for determining critical and essential workload				X	
team member responsibilities in responding to an emergency situation				X	
G. NSTISS Policies and Procedures (Performance Level)					
Instructional Content					
List and describe: elements of vulnerability and threat that exist in an AIS/telecommunications system with corresponding protection measures					X
List and describe: specific technological, policy, and educational solutions for NSTISS					X
(1) Topical Content					
(a) Physical Security Measures					

alarms					X
building construction					X
cabling					X
communications centers					X
environmental controls (humidity and air conditioning)					X
filtered power					X
Fire Protection		X			
information systems centers					X
physical access control systems (key cards, locks and alarms)		X			X
power controls (regulator, uninterrupted power service (UPS), and emergency poweroff switch)					X
protected distributed systems					X
shielding					X
stand-alone systems and peripherals					X
storage area controls		X			X
(b) Personnel Security Practices and					
access authorization/verification (need to know)					X
contractors		X			X
employee clearances		X			X
position sensitivity					X
security training and awareness		X			X
systems maintenance personnel					X
(c) Software Security					
assurance		X			
configuration management (change controls)		X			
configuration management (documentation)		X			
configuration management (programming standards and controls)		X			
software security mechanisms to protect information (access privileges)		X			

software security mechanisms to protect information (application security features)		X			
software security mechanisms to protect information (audit trails and logging)		X			
software security mechanisms to protect information (concept of least privilege)		X			
software security mechanisms to protect information (identification and authentication)		X			
software security mechanisms to protect information (internal labeling)		X			
Software Security Mechanisms to Protect Information (malicious logic protection)		X			
software security mechanisms to protect information (need to know controls)		X			
software security mechanisms to protect information (operating systems security features)		X			
software security mechanisms to protect information (segregation of duties)		X			
(d) Network Security					
dial up vs dedicated	X				
end-to-end access control	X				
privileges (class, nodes)	X				
public vs private	X				
traffic analysis	X				
(e) Administrative Security Procedural					
attribution		X		X	
construction, changing, issuing and deleting passwords		X		X	
copyright protection and licensing				X	
destruction of media		X		X	X
documentation, logs and journals				X	

emergency destruction				X	X
external marking of media		X		X	X
media downgrade and declassification		X		X	X
preperation of security plans				X	
reporting of computer misuse or abuse		X		X	
repudiation		X		X	
sanitization of media		X		X	X
transportation of media		X		X	X
(f) Auditing and Monitoring					
conducting security reviews			X	X	
effectiveness of security programs			X	X	
investigation of security breaches			X	X	
monitoring systems for accuracy and abnormalities			X	X	
privacy			X	X	
review of accountability controls			X	X	
review of audit trails and logs			X	X	
review of software design standards				X	
verification, validation, testing, and evaluation processes				X	
(g) Cryptosecurity					
cryptovariable or key		X			
electronic key management system		X			
encryption/decryption method, procedure, algorithm		X			
(h) Key Management		X			
access, control and storage of COMSEC material		X			
destruction procedures for COMSEC material		X			
identify and inventory COMSEC mateial		X			
key management protocols (bundling, electronic key, over-the-air rekeying)		X			
report COMSEC incidents		X			
(I) Transmission Security					

burst transmission	X				
covert channel control (crosstalk)	X				
dial back	X				
directional signals	X				
frequency hopping	X				
jamming	X				
line-of-sight	X				
line authentication	X				
low power	X				
masking	X				
optical systems	X				
protected wireline	X				
screening	X				
spread spectrum transmission	X				
(j) TEMPEST Security		X			
attenuation		X			
banding		X			
cabling		X			
filtered power		X			
grounding		X			
shielding		X			
TEMPEST seperation		X			
zone of control/zoning		X			