

CNSSI 4014 for NJCU

CNSSI 4014 Curriculum Map to NJCU Courses

Completed by: *Dr. John W. Collins, Jr.*

As of: 8/30/2007

	SECU 610	SECU 655	SECU 660	SECU 665
1. DEVELOP CERTIFICATION AND ACCREDITATION POSTURE				
A. PLANNING FOR CERTIFICATION AND ACCREDITATION				
(1) Planning				
*E - Define certification and accreditation		3.1		
E - Explain Common Criteria (CC)		3.1		
E - Discuss National Information Assurance Program (NIAP) Validated Products List		3.1		
E - Explain Information Technology Security Evaluation Criteria (ITSEC)		3.1		
E - Explain International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799		3.1		
E - Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)		3.1		
E - Discuss goals, mission, and objectives of the organization(s)		3.1		
E - Discuss Information Technology Security Evaluation Criteria (ITSEC)		3.1		
E - Discuss the concepts of availability, integrity, confidentiality, authentication, and non-repudiation		3.1		
E - Discuss the theoretical concepts of security models - confidentiality models (e.g., Bell & LaPadula)		3.1		
E - Discuss the theoretical concepts of security models - commercial systems models		3.1		
E - Discuss the theoretical concepts of security models - integrity models (e.g., Biba, Clark and Wilson)		3.1		
E - Discuss the theoretical concepts of security models - information flow models		3.1		
E - Discuss the components of information systems evaluation models		3.1		
E - Discuss the constituent components of the certification and accreditation process		3.1		
(2) Defense in Depth		9.1		
*E - Give examples of defense in depth methods				
(3) Assets				
*E - Define assets			3.3	
E - Define contracts, agreements, and other obligation policy			3.3	
E - Define policy for user roles			3.3	
E - Define system owner			3.3	
E - Define data owner			3.3	

CNSSI 4014 for NJCU

E - Discuss user roles			3.3
E - Identify assets			3.3
E - Identify contracts, agreements, and other obligations			3.3
E - Identify database structure			3.3
E - Identify system owner			3.3
E - Identify data owner			3.3
E - Identify systems interconnection			3.3
(4) Threats			
*E - Define adversarial threat			3.1
E - Define aggregation			3.1
E - Define technological threats			3.1
E - Define threats from careless/disgruntled employees			3.1
E - Define social engineering threats			3.1
E - Describe how espionage (industrial/international) can impact security of information systems			3.1
E - Describe adversarial threat			3.1
E - Describe how people can threaten system's security, i.e., intentional and unintentional			3.1
E - Describe how security reviews can be used to identify threats to information systems			3.1
E - Describe threat from electronic emanations			3.1
E - Describe threat from natural sources (fire, flood, earthquake, etc)			3.1
E - Describe types of environmental control (air conditioning, filtered power, etc.) threats			3.1
E - Describe types of intentional human threats to system			3.1
E - Describe types of unintentional human threats to system			3.1
E - Discuss aggregation			3.1
E - Discuss boundary			3.1
E - Discuss application and system vulnerabilities and threats - web-based (e.g., XML, SAML)			3.1
E - Discuss security implications posed by portable devices and components			3.1
E - Discuss application and system vulnerabilities and threats - client-based (e.g., applets, Active-X)			3.1
E - Discuss natural disaster impacts on system			3.1
E - Discuss application and system vulnerabilities and threats - server-based			3.1
E - Discuss application and system vulnerabilities and threats - mainframe			3.1
viruses, worms)			3.1
E - Discuss data mining			3.1
E - Discuss databases and data warehousing vulnerabilities, threats and protections			3.1
E - Discuss inference			3.1
E - Discuss object reuse			3.1
E - Discuss polyinstantiation			3.1
E - Discuss perimeter and building grounds protection issues/systems			3.1
E - Discuss access control attacks (brute force, dictionary, spoofing, denial of service, etc.)			3.1

CNSSI 4014 for NJCU

E - Discuss how the security architecture is affected by assurance and confidence			3.1
E - Discuss how the security architecture is affected by covert channels			3.1
E - Discuss how the security architecture is affected by countermeasures			3.1
E - Discuss how the security architecture is affected by emanations			3.1
E - Discuss how the security architecture is affected by maintenance hooks and privileged programs			3.1
E - Discuss how the security architecture is affected by resource misuse prevention			3.1
E - Discuss how the security architecture is affected by states attacks (e.g., time of check/time of use)			3.1
E - Discuss how the security architecture is affected by timing attacks			3.1
E - Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)			3.1
E - Identify appropriate EMSEC/TEMPEST authorities			3.1
E - Identify process for evaluating threat			3.1
E - Identify related disciplines that should contribute to risk analysis			3.1
(5) Vulnerabilities			
*E - Assist in performance of vulnerability analysis			3.5
E - Define National Information Assurance Program (NIAP) Validated Products List			3.5
E - Define Protection Profiles			3.5
E - Define vulnerabilities			3.5
E - Describe agency/vendor cooperation/coordination			3.5
E - Describe agency policy for access by uncleared individuals and vendors			3.5
E - Describe agency policy for redeploying classified systems			3.5
E - Describe technical surveillance vulnerabilities			3.5
E - Describe vulnerability analysis			3.5
E - Identify technical surveillance vulnerabilities			3.5
(6) Criticality			
*E - Define asset criticality			3.2
E - Define attack analysis			3.2
E - Define criticality			3.2
(7) Risk			
*E - Define risk (threat and vulnerability pairs together with significance)			3.3
E - Discuss risk management concepts			3.3
(8) Conduct Risk Assessment			
*E - Define information valuation			11.1

CNSSI 4014 for NJCU

E - Define risk assessment			11.1	
E - Describe risk assessment process			11.1	
E - Describe three states of information			11.1	
(9) Countermeasures				
*E - Define countermeasures			13.1	
E - Describe how countermeasures can mitigate risk			13.1	
E - Discuss application environment and security controls			13.1	
E - Discuss audit trails/access logs & intrusion detection applications			13.1	
E - Discuss firewalls			13.1	
E - Discuss badging, and smart/dumb cards			13.1	
E - Discuss biometric access controls to facility			13.1	
E - Discuss CCTV requirements/capabilities			13.1	
E - Define National Information Assurance Program (NIAP) Validated Products List			13.1	
E - Discuss escort requirements/visitor control issues			13.1	
E - Discuss fire detection and suppression issues/systems			13.1	
E - Discuss intrusion detection system (e.g., firewalls, motion detectors, sensors, alarms) requirements/capabilities			13.1	
E - Discuss keys and locks requirements/capabilities			13.1	
E - Discuss power and HVAC considerations			13.1	
E - Discuss restricted areas/work areas security requirements			13.1	
E - Discuss risk management concepts			13.1	
E - Discuss security guard requirements			13.1	
E - Discuss site selection and facility design configuration considerations			13.1	
E - Discuss turnstiles and mantraps requirements			13.1	
E - Discuss water, leakage, flooding impact to system			13.1	
E - Identify countermeasures to deter/mitigate attack threats (e.g.; malicious code, flooding, spamming)			13.1	
(10) Organizational/Agency Systems Emergency/Incident Response Team				
*E - Define organizational/agency systems emergency/incident response team		13.1		
E - Identify organizational/agency systems emergency/incident response team		13.1		
(11) Education, Training, & Awareness (ETA)				
*E - List topics for inclusion into education, training, and awareness (ETA) policy				11.2
E - Discuss ETA as a countermeasure				11.2
(12) Residual Risk				

CNSSI 4014 for NJCU

*E - Define residual risk			11.1	
(13) Cost/Benefit Analysis				
*E - Define cost/benefit analysis			11.1	
E - Define risk acceptance			11.1	
B. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA) POLICY				
(1) Contingency Plans				
*E - Define contingency plans	12.1			
E - Identify items for which plans must be developed	12.1			
E - Prepare input to contingency plan	12.1			
E - Write contingency plan	12.1			
(2) Concept of Operations (CONOP)				
*E - Define Concept Of Operations (CONOP)				4.2
(3) Continuity Plans				
*E - Define continuity plan	13.1			
E - Discuss business continuity planning (BCP)	13.1			
E - Discuss business organization analysis	13.1			
E - Discuss disaster recovery planning (DRP) (recovery planning and strategy)	13.1			
E - Discuss project scope development and planning	13.1			
E - Discuss resource requirements	13.1			
E - Identify items for which plans must be developed	13.1			
E - Outline security policy for backup procedures	13.1			
E - Prepare input to continuity plan	13.1			
E - Write continuity plan	13.1			
(4) Legal Plan				
*E - Discuss evidence collection and handling		14.1		
E - Discuss incident handling and response		14.1		
E - Discuss the parameters of investigations		14.1		

CNSSI 4014 for NJCU

*E - Discuss Clinger-Cohen Act		14.1		
E - Discuss Computer Fraud and Abuse Act		14.1		
E - Discuss Copyright Act of 1976		14.1		
E - Discuss Copyright Protection and License		14.1		
E - Discuss Electronic Freedom of Information Act		14.1		
E - Discuss Electronic Records Management and Federal Records Act		14.1		
E - Discuss Federal Information System Management Act		14.1		
E - Discuss Federal Managers Financial Integrity Act		14.1		
E - Discuss Federal Property and Administration Service Act		14.1		
E - Discuss Freedom of Information Act		14.1		
E - Discuss Government Paperwork Elimination Act		14.1		
E - Discuss Government Information Security Reform Act		14.1		
E - Discuss Millennium Copyright Act		14.1		
E - Discuss National Archives and Records Act		14.1		
E - Discuss Privacy Act issues		14.1		
E - Discuss USA Patriot Act		14.1		
E - Discuss computer crime and various methods used to commit computer crime		14.1		
E - Discuss computer crime laws		14.1		
E - Discuss implications of the Privacy Act		14.1		
E - Discuss import/export laws		14.1		
E - Discuss information systems security laws		14.1		
E - Discuss intellectual properties laws		14.1		
E - Discuss international legal issues which can affect information assurance		14.1		
E - Discuss liability laws		14.1		
E - Discuss licensing laws		14.1		
E - Discuss legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.		14.1		
E - Discuss requirements of Computer Security Act		14.1		
E - Discuss trans-border data flow laws		14.1		
(5) Disposition of Classified Material & Emergency Destruction Policy (EDP)				
*E - Define disposition of classified material				4.5
E - Explain emergency destruction policy (EDP) to those who execute plans				4.5
(6) Identification and Authentication (I&A) Policy				
*E - Discuss authentication		5.2		
E - Discuss non-repudiation		5.2		
E - Define account management		5.2		
E - Define authentication		5.2		

CNSSI 4014 for NJCU

E - Define biometrics	5.2			
E - Define identification and authentication (I&A)	5.2			
E - Define non-repudiation	5.2			
E - Define peer-to-peer security	5.2			
E - Define unauthorized access	5.2			
E - Describe how to choose appropriate passwords, and how/why to protect them	5.2			
E - Explain need for account management	5.2			
E - List underlying account management principles	5.2			
E - List underlying authentication principles	5.2			
E - List underlying security concerns with password sharing	5.2			
E - Discuss good passwords/password conventions	5.2			
(7) Monitoring and Auditing Policy				
*E - Define electronic monitoring			7.1	
E - Define intrusion detections			7.1	
E - Define keystroke monitoring			7.1	
E - Define keystroke monitoring requirements for policy and procedures			7.1	
E - Define monitoring			7.1	
E - Define required audit features			7.1	
E - Define requirements for error logs/system logs			7.1	
E - Describe audit collection requirements			7.1	
E - Describe policy for audit			7.1	
E - Identify audit and log tools			7.1	
E - Identify error and system tools			7.1	
E - Outline known means of electronic monitoring			7.1	
E - Outline known means of keystroke monitoring			7.1	
C. CONTROL SYSTEMS POLICIES				
(1) Configuration Management Policy				
*E - Define configuration management				6.1
E - Define Configuration Control Board (CCB)				6.1
(2) Protective Technology Policy				
*E - Define protective technology				6.2
E - List protective technologies				6.2

CNSSI 4014 for NJCU

(3) Intrusion Detection Policy			
*E - Define intrusion detection			4.1
(4) Malicious Code Policy			
*E - Define malicious code			4.2
E - Describe malicious code and outline various types of malicious code			4.2
E - Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)			4.2
(5) Access Controls			
*E - Define need to understand policy		9.2	
E - Define need-to-know		9.2	
E - Define risk management policy		9.2	
E - Explain user access policy		9.2	
E - Explain user access requirements		9.2	
D. CULTURE AND ETHICS			
(1) Policy			
*E - Define culture and ethics policy			14.2
E - Define roles, responsibilities, and organization (e.g., separation of duties)			14.2
E - Identify basic management issues and their impact on information systems security program			14.2
(2) Organization Culture			
*E - Describe organization culture			14.1
(3) Basic/Generic Management Issues			
*E - Describe basic/generic management issues			14.1
(4) Agency-Specific Security Policies & Procedures			
*E - Describe how effective security policies and procedures can reduce threats to information systems			14.2

CNSSI 4014 for NJCU

E - Identify security policy-making bodies			14.2	
E. INCIDENT RESPONSE				
(1) Concept of Operations (CONOP)				
*E - Define Concept of Operations (CONOP)				4.2
(2) Criminal Activity Preparedness Planning				
*E - Explain criminal activity preparedness planning policy				4.3
(3) Organizational/Agency Systems Emergency/Incident Response Team				
*E - Define organizational/agency systems emergency/incident response team				4.1
E - Identify organizational/agency systems emergency/incident response team				4.1
E - Interact with organizational/agency systems emergency/incident response team to resolve incidents				4.1
(4) Malicious Code				
*E - Define malicious code			4.3	
E - Describe malicious code and outline various types of malicious code			4.3	
E - Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)			4.3	
2. IMPLEMENT SITE SECURITY POLICY				
A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)				
(2) Emergency Destruction Procedures (EDP)				
*E - Discuss current emergency destruction plan (EDP) with necessary parties				4.5
(3) Continuity Plans				
*E - Address recovery procedures with SA/staff				4.3
*E - Define who has responsibility for accountability				4.3
E - Describe accounting process for hardware, software, and information				4.3
E - Outline accountability process/program				4.3

CNSSI 4014 for NJCU

(4) Disposition of Classified Material				
*E - Address disposition procedures with system administrator SA/staff			2.1	
E - Explain the maintenance of audit records			2.1	
(5) Monitoring and Auditing				
*E - Address auditing and logging management with SA/staff			7.1	
E - Address work force auditing and logging management procedures			7.1	
E - Discuss alarms, signals, and reports requirements			7.1	
E - Discuss auditing and logging management policies, laws, and penalties with personnel			7.1	
E - Discuss current auditing and logging management with necessary parties			7.1	
(7) Intrusion Detection				
*E - Address intrusion detection management with SA/staff			13.1	
E - Address SA/staff about monitoring and auditing intrusion detection policies			13.1	
E - Address work force about intrusion detection management procedures			13.1	
(8) Investigation of Security Breaches				
*E - Define security breaches			12.3	
(9) Monitoring				
*E - Address monitoring management with SA/staff			7.1	
E - Address SA/staff about legal monitoring restrictions			7.1	
E - Address work force about monitoring management procedures			7.1	
(10) Configuration Management				
*E - Address configuration management with SA/staff				6.1
E - Address SA/staff about legal configuration restrictions				6.1
E - Address work force about configuration management procedures				6.1
(11) Countermeasures				
*E - Discuss intrusion detection problems			13.1	
*E - Define cryptanalytic techniques			13.1	

CNSSI 4014 for NJCU

E - Define cryptographic concepts			13.1	
E - Define digital signatures/non-repudiation			13.1	
E - Define key management			13.1	
E - Define message digests (e.g., MD5, SHA, HMAC)			13.1	
E - Define methods of encryption			13.1	
E - Identify protective technologies			13.1	
B. ENSURE FACILITY IS APPROVED				
(Not Categorized)				
*E - Define an approved facility			3.1	
E - Define an approved service			3.1	
C. OPERATIONS				
(2) Agency/Vendor Cooperation/Coordination				
*E - Describe agency policy for redeploying classified systems to the SA and SSM viz., CIO, DAA, CTO, etc.			13.1	
E - Explain agency policy for access by uncleared individuals and vendors to the SA and SSM viz., CIO, DAA, CTO, etc.			13.1	
E - Explain cooperation concerns to vendors			13.1	
E - Explain cooperation concerns with vendors to SSM, viz., CIO, DAA, CTO, etc.			13.1	
E - Facilitate agency control of access by uncleared individuals and vendors			13.1	
E - Facilitate correct agency redeployment of classified systems			13.1	
E - Facilitate vendor cooperation			13.1	
(3) Certification Advocacy				
*E - Define advocacy			2.1	
E - Explain advocacy role			2.1	
(4) Conduct Risk Assessment				
*E - Define information valuation			11.1	
E - Define risk assessment			11.1	
E - Describe risk assessment process			11.1	
E - Describe three states of information			11.1	
(5) Contracting for Security Services				

CNSSI 4014 for NJCU

*E - Define an approved service				13.1
E - Explain security services to contracting officers				13.1
(7) Life Cycle System Security Planning				
*E - Define life cycle security			5.1	
E - Describe agency policy for redeploying classified systems			5.1	
E - Explain life cycle security planning			5.1	
E - Explain life cycle system security planning			5.1	
(8) System Security Architecture Study				
*E - Address system security architecture study			6.1	
E - Define system security architecture			6.1	
E - Explain system security architecture study			6.1	
D. GENERAL PRINCIPLES				
(1) Access Control Models				
*E - Discuss access control models		5.3		
(2) Approval to Operate				
*E - Explain approval to operate			3.1	
(3) Attack				
				4.2
*E - Explain attack				4.2
E - Explain backdoor routines				4.2
E - Explain denial-of-service (DOS) attacks				4.2
E - Explain remote explorer attack				4.2
E - Explain attack root exploits				4.2
E - Explain session hijacking tools				4.2
E - Explain war dialer/THC-scan attacks				4.2
E - Explain war dialers				4.2
(4) Business Aspects of Information Security				

CNSSI 4014 for NJCU

*E - Explain business aspects of information security		2.1		
(6) Computer Network Attack				
*E - Explain computer network attack			4.2	
(7) Criminal Prosecution				
*E - Explain criminal prosecution		10.2		
(8) Defense in Depth				
*E - Give examples of defense in depth methods		9.1		
(9) Due Care				
*E - Address questions from users about due care		9.2		
E - Monitor adherence to due care rules		9.2		
E - Remind users of due care rules		9.2		
(10) Education, Training, & Awareness				
*E - List topics for inclusion into education, training and awareness plan				11.1
E - Recognize AT&E is a countermeasure				11.2
(11) Industrial Security				
*E - Explain industrial security				13.1
(12) Information Warfare (INFOWAR) Concepts				
*E - Explain INFOWAR concepts	11.1			
(13) Intellectual Property Rights				
*E - Explain intellectual property rights	10.1			
(14) Interim Approval to Operate (IATO)				
*E - Explain interim approval to operate		3.1		

CNSSI 4014 for NJCU

(15) Investigative Authorities				
*E - Explain investigative authorities			12.3	
(16) Knowledge of Security Laws				
*E - Discuss Clinger-Cohen Act	14.1			
E - Discuss Computer Fraud and Abuse Act	14.1			
E - Discuss Computer Security Act	14.1			
E - Discuss Copyright Law of the United States and related laws	14.1			
E - Discuss Copyright protection and licenses	14.1			
E - Discuss Electronic Freedom of Information Act	14.1			
E - Discuss Electronic Records Management and Federal Records Act	14.1			
E - Discuss Federal Information System Management Act	14.1			
E - Discuss Federal Managers Financial Integrity Act	14.1			
E - Discuss Federal Property and Administration Service Act	14.1			
E - Discuss Freedom of Information Act	14.1			
E - Discuss Government Paperwork Elimination Act/Paperwork Reduction Act	14.1			
E - Discuss Government Information Security Reform Act	14.1			
E - Discuss Millennium Copyright Act	14.1			
E - Discuss National Archives and Records Act	14.1			
E - Discuss Privacy Act/Privacy Act issues	14.1			
E - Discuss USA Patriot Act	14.1			
E - Discuss computer crime and the various methods	14.1			
E - Discuss international legal issues which can affect Information Assurance	14.1			
E - Discuss the legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.	14.1			
(17) Lattice Model				
*E - Define lattice model	2.1			
(18) Law Enforcement Interfaces				
*E - Explain law enforcement interfaces		13.1		
(20) Need for System Certification				
*E - Explain need for system certification		3.1		

CNSSI 4014 for NJCU

(21) Operating Security Features				
*E - Explain operating security features				12.1
(22) Risk Management				
*E - Explain risk management		11.1		
(23) Security Awareness as a countermeasure				
*E - Define security awareness for information system users				11.1
(24) Security Education as a countermeasure				
*E - Encourage employees to seek education in IA as a countermeasure				11.2
(25) Security Training as a countermeasure				
*E - Define security training for information system users				11.2
(26) Software Licensing				
*E - Explain software licensing		14.2		
(27) Software Piracy				
*E - Explain software piracy		14.3		
(28) Systems Security Authorization Agreement (SSAA)				
*E - Explain SSAA				13.1
(29) Systems Security Plan (SSP)				
*E - Explain Systems Security Plan (SSP)	2.1			
(30) Standards of Conduct				
*E - Explain standards of conduct				14.1

CNSSI 4014 for NJCU

(32) Waive Policy to Continue Operation				
*E - Explain Waive Policy to Continue Operation				4.3
E. SECURITY MANAGEMENT				
(1) Electronic Records Management				
*E - Define electronic records management program and tools		2.2		
E - Define underlying rules for electronic records management program		2.2		
E - Describe the effect of electronic records management on the system		2.2		
(2) Records Retention				
*E - Discuss electronic records retention program		2.2		
E - Define underlying rules for electronic records retention program		2.2		
E - Describe effect of records retention system		2.2		
E - List use of record retention		2.2		
(3) E-Mail				
*E - Address SA/staff about legal e-mail monitoring restrictions		2.2		
E - Describe e-mail retention policies as they apply to system		2.2		
E - Describe e-mail system/e-mail system security		2.2		
E - Describe e-mail system and its potential vulnerabilities		2.2		
E - Explain e-mail monitoring management with SA/staff		2.2		
E - Discuss appropriate laws and policies for e-mail monitoring		2.2		
(4) Non-Repudiation				
*E - Describe non-repudiation and its application to system		14.1		
(5) Hardware Asset Management				
*E - Describe agency policy for access by uncleared individuals and vendors		11.2		
E - Describe agency policy for redeploying classified systems		11.2		
E - Describe hardware asset management program		11.2		
E - Describe hardware asset management program and how it applies and is used on the system		11.2		
(6) Software Asset Management				

CNSSI 4014 for NJCU

*E - Describe agency policy for access by uncleared individuals and vendors		11.2		
E - Describe agency policy for redeploying classified systems		11.2		
E - Describe software asset management program		11.2		
E - Describe software asset management program and how it applies and is used on the system		11.2		
E - Describe software asset management program and how it applies/is used on system with emphasis on license and copyright issues, and cross reference to ethics		11.2		
F. ACCESS CONTROLS				
(1) Human Access				
*E - Address access management with SA/staff				5.3
E - Address SA/staff about legal access restrictions				5.3
E - Address work force about access management procedures				5.3
E - Describe agency policy for access by uncleared individuals and vendors				5.3
E - Address access management with SA/staff				5.3
E - Address SA/staff about legal access restrictions				5.3
E - Address work force about access management procedures				5.3
*E - Address access control software management with SA/staff				5.3
E - Address SA/staff about legal access restrictions				5.3
E - Address work force about access control software management procedures				5.3
E - Discuss access control software management policies, laws and penalties with personnel				5.3
E - Discuss current access control software management with necessary parties				5.3
*E - Address account management with SA/staff				5.3
E - Address work force about account management procedures				5.3
*E - Address authentication with SA/staff				5.3
E - Address work force about authentication procedures				5.3
E - Discuss authentication policies, laws, and penalties with personnel				5.3
E - Discuss current authentication with necessary parties				5.3
*E - Address biometric access management with SA/staff				5.3
E - Discuss biometric access management policies, laws and penalties with personnel				5.3
E - Discuss current biometric access management with necessary parties				5.3
*E - Address password management with SA/staff				5.3
E - Address work force authentication procedures				5.3
E - Discuss current password management with necessary parties				5.3
E - Discuss password management policies, laws, and penalties with personnel				5.3
*E - Address unauthorized access incident reporting with SA/staff				5.3
E - Discuss unauthorized access policies, laws, and penalties with personnel				5.3

CNSSI 4014 for NJCU

(2) Key Management				
*E - Explain to users and managers what COMSEC process is and how COMSEC process is relevant to them			2.1	
E - Identify COMSEC			2.1	
E - Identify use for COMSEC material on system			2.1	
E - Integrate services and advice of COMSEC Manager (Custodian) with operations			2.1	
E - List national COMSEC policies			2.1	
E - List national COMSEC procedures			2.1	
*E - Define EKMS			2.1	
E - Demonstrate knowledge of how to operate an EKMS system			2.1	
E - Describe to users and managers what EKMS is, and how/why it is used			2.1	
E - Describe to users and managers what key management is, and how/why EKMS is used			2.1	
E - Identify components of EKMS as it applies to system			2.1	
E - Identify EKMS requirements			2.1	
E - Outline EKMS national policies and procedures and explain their relevance to users			2.1	
E - Outline EKMS policies and procedures and explain their relevance to users			2.1	
E - Outline national & agency EKMS management policies and procedures, and explain their relevance to users			2.1	
E - Submit EKMS requirements			2.1	
E - Use EKMS management in a system			2.1	
*E - Describe to users and managers what key escrow is, and how/why it is used			2.1	
E - Explain national key escrow policies and procedures			2.1	
E - Use key escrow management in a system			2.1	
*E - Define KMI			2.1	
*E - Define peer-to-peer			2.1	
E - Identify peer-to-peer requirements			2.1	
*E - Define Public Key Infrastructure (PKI)			2.1	
E - Demonstrate knowledge of how to operate a PKI system			2.1	
E - Describe to users and managers what key management is, and how/why PKI is used			2.1	
E - Describe to users and managers what PKI is, and how/why it is used			2.1	
E - Identify components of PKI as it applies to system			2.1	
E - Identify PKI requirements			2.1	
E - Outline national & agency PKI management policies and procedures, and explain their relevance to users			2.1	
E - Outline PKI national policies and procedures and explain their relevance to users			2.1	
E - Outline PKI policies and procedures and explain their relevance to users			2.1	
E - Submit PKI requirements			2.1	
E - Use PKI management in a system			2.1	
G. INCIDENT RESPONSE				

CNSSI 4014 for NJCU

Security Investigation Procedures				
*E - Assist in investigations as requested			12.3	
E - Describe process of investigating security incident			12.3	
E - Follow procedures			12.3	
E - Identify investigating authorities			12.3	
3. ENFORCE AND VERIFY SYSTEM SECURITY POLICY				
A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY/ACCOUNTABILITY (CIA)				
(1) Planning				
*E - Discuss continuity plans				4.1
*E - Discuss contingency plans				4.1
*E - Discuss reconstitution plans				4.1
*E - Discuss disposition of classified material & EDP				4.1
(2) Monitoring and Auditing				
*E - Discuss alarms, signals, and reports requirements			7.1	
*E - Discuss intrusion detection problems			7.1	
*E - Discuss security breaches			7.1	
E - Define security breach			7.1	
*E - Define keystroke monitoring			7.1	
E - Ensure legal requirements for monitoring are enforced			7.1	
E - Identify potential monitoring problems			7.1	
*E - Discuss network monitoring problems			7.1	
E - Explain consequences of unapproved monitoring			7.1	
(3) Environmental Controls				
*E - Discuss environmental control issues			9.1	
(4) Filtered Power				
*E - Discuss filtered power issues			9.1	
(5) Fire Prevention				

CNSSI 4014 for NJCU

*E - Discuss fire prevention issues			9.1	
(6) Grounding				
*E - Discuss grounding issues			9.1	
(7) Safety				
*E - Discuss safety issues			9.1	
C. ACCESS CONTROLS				
(1) Human Access				
*E - #Require users and system support personnel to have required security clearances, authorizations and need-to-know, and are indoctrinated before granting access	5.3			
E - Describe agency policy for access by uncleared individuals and vendors	5.3			
*E - Verify requested access	5.3			
*E - Discuss unauthorized access attempts	5.3			
(2) Key Management				
*E - List national COMSEC policies	5.3			
E - List national COMSEC procedures	5.3			
*E - Explain national key escrow policies and procedures	5.3			
(3) Configuration Management				
*E - Identify configuration management requirements				6.1
(4) Protective Technology				
*E - Identify protective technology requirements			6.1	
D. AUTOMATED SECURITY TOOLS				
(1) Automated Security Tools				
*E - Use expert system tools (i.e., audit reduction and intrusion detection) available			7.1	

CNSSI 4014 for NJCU

E. HANDLING MEDIA				
(6) Remanence				
*E - Execute non-automated data remanence tools			9.1	
(8) Disposition of Classified Material				
*E - Explain disposition of classified media policies and procedures			6.2	
E - Define disposition reports			6.2	
F. INCIDENT RESPONSE				
(1) Criminal Prosecution				
*E - Discuss criminal prosecution requirements				10.3
(4) Legal and Liability Issues				
*E - Discuss legal liability issues		14.1		
E - Identify legal liability issues		14.1		
4. REPORT ON SITE SECURITY STATUS				
A. SECURITY CONTINUITY REPORTING				
(1) Contingency Plans				
*E - Define contingency plan reporting				4.1
(2) Continuity Plans				
*E - Define continuity plan reporting				4.3
E - Define reconstitution reporting				4.3
*E - Define restoration reports				4.3
E - Define backup reports				4.3
(3) Disposition of Classified Material & Emergency Destruction Procedures (EDP)				

CNSSI 4014 for NJCU

*E - Define disposition reports			6.1	
E - Define EDP reports			6.1	
(4) Monitoring and Auditing				
*E - Explain reporting audit alarms and signals			7.1	
*E - Explain how to report audit assessments			7.1	
(5) Identification & Authentication				
*E - Describe process to report unauthorized accounts				5.1
*E - Describe process to report insufficient passwords				5.1
(6) Configuration Management				
*E - Describe configuration management reporting requirements				6.1
(7) Testing				
*E - Describe how various types of testing are reported		5.1		
B. REPORT SECURITY INCIDENTS				
(1) Computer Organizational/Agency Systems Emergency/Incident Response Team				
*E - Identify organizational/agency systems emergency/incident response team		10.3		
E - Distribute organizational/agency systems emergency/incident response team reports and advisories		10.3		
(3) Security Violations Reporting Process (incident response)				
*E - Comply with agency specific/local directives when reporting to SSM, viz., CIO, DAA, CTO, etc.		10.3		
C. LAW				
(1) Investigative Authorities				
*E - Identify agencies and offices responsible for investigating security incidents		13.1		
(2) Law Enforcement Interfaces (LEI)				

CNSSI 4014 for NJCU

*E - Describe how ISSO interfaces with law enforcement agencies		13.1		
E - Describe how to contact law enforcement interfaces (LEI)		13.1		
(3) Witness Interviewing/Interrogation				
*E - Assist appropriate authority in witness interviewing/interrogation			12.3	
E - Describe proper procedures to follow when conducting a witness interview			12.3	
E - Identify who can conduct interrogations (investigative agencies only)			12.3	
(5) Disgruntled Employees				
*E - Identify notification requirements for handling disgruntled employees				5.2
D. REPORT SECURITY STATUS OF INFORMATION SYSTEM AS REQUIRED BY SSM, VIZ., CIO, DAA, CTO, ETC.				
(1) Administrative Security Policies and Procedures				
*E - Explain necessity of reporting on administrative security policies and practices				13.1
(2) Agency Specific Security Policies				
*E - Describe how agency specific policies enhance overall security posture of information systems by defining operational environment				13.1
(3) Organizational/Agency Systems Emergency/Incident Response Team				
*E - Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems				13.1
(4) Automated Systems Security Incident Support Team (ASSIST)				
*E - Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems			10.1	
(5) Trade Journals, Bulletin Board System (BBS) Notices				
*E - Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems			10.1	

CNSSI 4014 for NJCU

E. REPORT TO IG				
Inspector General (IG) (External) Audit & Assessments				
			10.3	
*E - Describe areas encompassed by report			10.3	
E - Identify appropriate reporting channels for IG				
5. SUPPORT CERTIFICATION AND ACCREDITATION				
A. CERTIFICATION FUNCTION				
(1) Assessments (e.g., surveys, inspections)				
*E - Prepare assessments for use during certification of information systems			3.1	
B. ACCREDITATION FUNCTION				
(1) ISSO				
*E - Monitor system status post accreditation			3.1	
E - Initiate accreditation process			3.1	
(3) System Administrator (SA)				
*E - Explain contents of Systems Security Plan (SSP)			3.1	
C. RESPOND TO SSM, VIZ., CIO, DAA, CTO, ETC. REQUESTS				
(1) Approval to Operate				
*E - Explain purpose and contents of Approval to Operate (ATO) to users			3.1	
(2) Assessment Methodology				
*E - Explain C&A process for information system			3.1	
(3) Certification Statement				
*E - Explain purpose and contents of Certification Statement to users			3.1	

CNSSI 4014 for NJCU

(4) Certification Tools				
*E - Discuss certification tools			3.1	
E - Discuss ST&E plan and procedures			3.1	
E - Recommend revisions to ST&E plan and procedures			3.1	
E - Recommend use of specific certification tools			3.1	
(5) Identify Security Changes to SSM, viz., CIO, DAA, CTO, etc.				
*E - Differentiate security-related changes from non-security-related changes			6.1	
E - Explain security-relevant changes to be made to information system			6.1	
(6) Interim Approval to Operate (IATO)				
*E - Explain purpose and contents of Interim Approval to Operate (IATO) to users			3.1	
(7) Re-Certification				
*E - Explain purpose and process of re-certification			3.1	
E - Identify information system that needs re-certification			3.1	
(8) Security Test & Evaluation (ST&E)				
*E - Discuss ST&E			5.1	
(9) SSAA				
*E - Explain contents of SSAA				12.3
(10) Type Accreditation				
*E - Explain purpose and contents of type accreditation to users			3.1	
(11) Waive Policy to Continue Operation				
*E - Explain justification for waiver			3.1	