CNSSI 4013 Entry Level Mapping to JSU Courses

Completed by: Dr. Guillermo A. Francia, III

As of: 08/08/2008

	CS 201	CS 232	CS 307	CS 310	CS 450	CS 462	CS 470
FUNCTION 1 - SECURE USE							
A. General Security Policy							
1. Accountability							
*E - Define organizational accountability policies			III,IV				
E - Outline accountability process/program			III,IV				
2. Accreditation							
*E - Define accreditation			VI.e				
3. Architecture							
*E - Define system security architecture							XV, XVI
E - Identify appropriate security architecture for use in assigned IS							XV, XVI
E - Address system security architecture study							XV, XVI
4. Assessment							
*E - Define assessments for use during certification of information systems			VII				
5. Assurance							
*E - Define assurance			I				I
6. Availability/Integrity/Confidentiality/Authentication/Non-repudiation							
*E - Define concepts of availability, integrity, confidentiality, authentication, and non-repudiation			I				I
7. Certification							
*E - Define certification policies as related to organizational requirements			VI.e				
8. NSTISSP 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA Enabled Information Technology (IT) Products							
*E - Identify NSTISSP 11 (Common Criteria) policies							XVIII
9. Configuration Control							
*E - Define configuration control (management)			II				
10. Custodian							
*E - Define resource custodian			X.d				
E _ Identify information resource custodian			X.d				
11. Defense in Depth							
*E - Define defense in depth			IX				
E _ Give examples of defense in depth methods			IX				
E - Give examples of defense in depth policy			IX				
12. Document							
*E - Identify DoDD 8500.1 policies (or appropriate civil agency guidance)			IV				III,IV,V
13. Domains							
*E - Define security domains as applicable to organizational policies			IV				III,IV,V
E - Describe security domains as applicable to organizational policies			IV				
14. E-Mail							
*E - Define organizational e-mail privacy policies	I.g		XI			V	
15. Wireless Security							
*E - Identify organizational wireless security policy			IX				XIV
16. EMSEC/TEMPEST (Emanations Security/Short name referring to the investigation, study, and control of compromising emanations from IS equipment)							
*E - Define EMSEC/TEMPEST security policies					III.h		
E - Describe EMSEC/TEMPEST control policies					III.h		
E - Identify EMSEC/TEMPEST control policies					III.h		
E - Identify EMSEC/TEMPEST security policies					III.h		
18. FAX							
*E - Describe relevant FAX security policies							XV.f
19. Generally Accepted Security Principles							
*E - Define generally accepted systems security principles			I,II				I, X, XV
20. Goals/Mission/Objectives							
*E - Define goals, mission, and objectives of the organization			II				
21. Incident Response							
*E - Describe incident response policies			VII, VIII				
22. Information Assurance							
*E - Define organizational Information Assurance (IA) policies			IV				III
23. Information Operations [DOD Organizations Only]							
*E - Define information operations							
E - Describe information operations							
E - Support information operations							
24. Internet Security							
*E - Describe organizational policies relevant to Internet security			XVII				
25. Law Enforcement							
*E - Identify law enforcement interfaces			III, XI				
E - Describe law enforcement interfaces			III, XI				
26. Marking							
*E - Define policies relating to marking of classified, unclassified and sensitive information			IV,XIII				IV,V,VI
27. Monitoring							
*E - Comply with legal aspects of monitoring			XI			V	XII
E - Ensure legal aspects of monitoring are enforced			XI			V	XII
28. Multi-Level Security							
*E - Describe multiple secure levels			IX				II, X, XI
E - Identify fundamental concepts of multilevel security							II, X, XI
E - Define fundamental concepts of multilevel security							II, X, XI
E - Describe fundamental concepts of multilevel security							II, X, XI
29. Network							
*E - Describe computer network defense			IV,IX				XIV
E - Describe policies relevant to network security			IV,IX				XIV
E - Describe wide area network (WAN) security policies			IV,IX				XIV
30. Operating System							
*E - Define functional requirements for operating system integrity							XV,XVI

32. Ownership								
*E - Define information ownership of data held under his/her cognizance				II				I
E - Identify information ownership of data held under his/her cognizance				II				I
E - Identify information resource owner				II				I
33. Physical Security								
*E - Define physical security				I, II				XIV
34. Records Management								
*E - Define records management				XI				XI
E - Describe organizational security policies relative to electronic records management				XI				XI
37. Security Tools								
*E - Define automated security tools				IV.g				XII-XIV
38. Sensitivity								
*E - Define information sensitivity								III-VI
E - Describe information sensitivity in relation to organizational policies								III-VI
E - Explain information sensitivity								III-VI
39. Separation of Duties								
*E - Define separation of duties				X				X
E - Explain separation of duties				X				X
E - Define organizational policies relating to separation of duties				X				X
40. System Security								
*E - Identify systems security standards policies				IV				XV
41. Information Technology Security Evaluation Criteria (ITSEC)								
*E- Identify Information Security Technology Security Evaluation Criteria (ITSEC) policies								XVIII.b
42. Testing								
*E - Define testing policies								XVI.e
43. Validation/Verification								
*E - Define validation policies								XVI.e
E - Identify verification and validation process policies								XVI.e
44. Workstation								
*E - Describe workstation security policies	I.g							XV
45. Zone								
*E - Define zone of control								XV.g
E - Define zoning								XV.g
E - Describe zoning and zone of control policies								XV.g
B. General Procedures								
1. Network Software								
*E - Define transport control protocol/internet protocol (TCP/IP)				IX		XVII		XIV
E - Define transport layer security (i.e., secure socket layer [SSL])				IX		XVII		XIV
E - Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)				IX		XVII		XIV
E - Define virtual private network (VPN) (i.e., SSH2, SOCKS)				IX		XVII		XIV
E - Describe secure e-mail (i.e., PGP, S/MIME)				IX		XVII		XIV
E - Describe secure systems operations procedures				IX		XVII		XIV
E - Describe transport control protocol/internet protocol (TCP/IP)				IX		XVII		XIV
E - Describe transport layer security (i.e., secure socket layer [SSL]				IX		XVII		XIV
E - Describe tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)				IX		XVII		XIV
E - Describe virtual private network (VPN) (i.e., SSH2, SOCKS)				IX		XVII		XIV
2. Aggregation								
*E - Define aggregation				IX				XIV
E - Describe aggregation				IX				XIV
3. Application Vulnerabilities								
*E - Describe application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)								XIII
E - Describe application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)								XIII
E - Describe application and system vulnerabilities and threats -- server-based								XIII
E - Describe application and system vulnerabilities and threats -- mainframe								XIII
E - Describe application and system vulnerabilities and threats -- malicious code (i.e., Trojan horses, trap doors, viruses, worms)	I.g							XIII
4. Architecture								
*E - Address system security architecture study								XVI
5. Assessment								
*E - Prepare assessments for use during certification of information systems				VI.e				XVIII
7. Organizational/Agency Systems Emergency Response Team								
*E - Identify organizational/agency systems emergency response team				II, III				
E - Report security issues to organizational/agency systems emergency response team				II, III				
8. Database								
*E - Define data mining								XV.h
E - Define databases and data warehousing vulnerabilities, threats and protections								XV.h
E - Describe data mining								XV.h
E - Describe databases and data warehousing vulnerabilities, threats and protections								XV.h
9. EMSEC/TEMPEST								
*E - Define EMSEC/TEMPEST security procedures						III.h		
E - Identify certified EMSEC/TEMPEST technical authority (CTTA)						III.h		
E - Identify EMSEC/TEMPEST security procedures						III.h		
10. End Systems								
*E - Define end systems (i.e., workstations, notebooks, PDA [personal digital assistant], smartphones, etc.)	I					I		
E - Describe end systems (i.e., workstations, notebooks, PDA, smartphones, etc.)	I					I		
11. Facility Management								
*E - Practice facility management procedures				II-IV				
12. FAX								
*E - Describe FAX security policies/procedures								XV.f
E - Practice FAX security policies/procedures								XV.f
13. Housekeeping								
*E - Define housekeeping procedures				IV-V				
E - Describe housekeeping procedures				IV-V				
E - Perform housekeeping procedures				IV-V				

14. Inference									
	*E - Define Inference								II,XV.h
	E - Describe Inference								II,XV.h
15. Information States									
	*E - Define information states procedures								I-III
	E - Describe information states procedures								I-III
16. Internet									
	*E - Define Internet security procedures	I.g		XVII					
17. Investigations									
	*E - Assist in investigations as requested			V-VI					
18. IPSEC									
	*E - Define IPSEC authentication and confidentiality					VI			XIV
	E - Describe IPSEC authentication and confidentiality					VI			XIV
19. Marking									
	*E - Perform marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example								IV,V,IX
20. Multi-Level Security									
	*E - Define multilevel security								II,X,XI
21. Network, General									
	*E - Define network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)					I			
	E - Define network components (hardware, firmware, software, and media)	I				I			
	E - Define network layer security					VI			XIV
	E - Define network protocols					VI			
	E - Define network types					I			
	E - Define wireless security					V			IX
	E - Describe network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)					I			
	E - Describe network components (hardware, firmware, software, and media)					I			
	E - Describe network layer security			IX		VI			XIV
	E - Describe network protocols					VI			
	E - Describe network types					I			
	E - Describe WAN security procedures					VI			
	E - Describe wireless security			IX					XIV
	E - Discuss network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)					I			
	E - Practice WAN security procedures			IX					XIV
22. Network Hardware									
	*E - Define cable characteristics (i.e., twisted pair, fiber)					I			
	E - Define concentrators					III			
	E - Define front-end processors, hubs, modems, multiplexers					III			
	E - Define gateways and routers					V			
	E - Define patch panels					III			
	E - Define routers					V			
	E - Define switches					V			
	E - Describe cable characteristics (i.e., twisted pair, fiber)					III			
	E - Describe concentrators					III			
	E - Describe front-end processors, hubs, modems, multiplexers					V			
	E - Describe gateways and routers					V			
	E - Describe patch panels					III			
	E - Describe routers					V			
	E - Describe switches					V			
	E - Identify gateways and routers					V			
23. Network Software									
	*E - Define firewall architecture (i.e., bastion host, DMZ)			IX					XIV
	E - Define firewall technology (i.e., packet filtering, data inspection)			IX					XIV
	E - Define secure e-mail (i.e., PGP, S/MIME)			IX					XIV
	E - Describe firewall architecture (i.e., bastion host, DMZ)			IX					XIV
	E - Describe firewall technology (i.e., packet filtering, data inspection)			IX					XIV
	E - Describe secure e-mail (i.e., PGP, S/MIME)			IX					XIV
	E - Identify firewall architecture (i.e., bastion host, DMZ)			IX					XIV
	E - Identify firewall technology (i.e., packet filtering, data inspection)			IX					XIV
	E - Identify secure e-mail (i.e., PGP, S/MIME)			IX					XIV
24. Objects									
	*E - Define object reuse		III		I.b, III.b				
	E - Define polyinstantiation		III		I.b, III.b				
	E - Describe object reuse		III		I.b, III.b				
	E - Describe polyinstantiation		III		I.b, III.b				
25. Operating System									
	*E - Define operating systems security procedures								XV-XVI
	E - Describe operating system integrity procedures								XV-XVI
	E - Perform operating systems security procedures								XV-XVI
26. OSI (Open Systems Interconnect)									
	*E - Define application layer security protocols (i.e., secure electronic transactions, secure hypertext, secure remote procedure call)								XIV.d
	E - Define data link layer security								XIV.d
	E - Define network layer security								XIV.d
	E - Define OSI model					I			XIV.d
	E - Define transport control protocol/ internet protocol (TCP/IP)					VII			XIV.d
	E - Define transport layer security (i.e., secure socket layer [SSL])								XIV.d
	E - Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)					VI			XIV.d
	E - Describe application layer security protocols (i.e., secure electronic transactions, secure hypertext, secure remote procedure call)								XIV.d
	E - Describe data link layer security								XIV.d
	E - Describe network layer security								XIV.d
	E - Describe OSI model					I			XIV.d
	E - Describe presentation layer					I			XIV.d
	E - Describe session layer					I			XIV.d
	E - Describe physical layer					I			XIV.d

			E - Describe transport control protocol/ internet protocol (TCP/IP)					I		XIV.d
			E - Describe transport layer security (i.e., secure socket layer [SSL])							XIV.d
		27. Rainbow Series								
			*E - Describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI) or Red Book as examples							XVIII
		28. NSTISSAM COMPUSEC/1-99								
			*E - Describe purpose and contents of NSTISSAM COMPUSEC/1-99, Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation							XVIII
		29. Security Procedures								
			*E - Define organizational security procedures			II-III				
			E - Assist in organizational security procedures			II-III				
		30. Security tools								
			*E - Define automated security tools			IV.g				
			E - Describe automated security tools			IV.g				
		31. Vulnerability and Threat								
			*E - Address application and system vulnerabilities and threats - mainframe			VII				XIII
			E - Address application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)			VII				XIII
			E - Address application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)			VII				XIII
			E - Address application and system vulnerabilities and threats -- server-based			VII				XIII
			E - Address application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)			VII				XIII
			E - Define application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)			VII				XIII
			E - Define application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)			VII				XIII
			E - Define application and system vulnerabilities and threats -- server-based			VII				XIII
			E - Define application and system vulnerabilities and threats -- mainframe			VII				XIII
			E - Define application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)			VII				XIII
			E - Describe application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)			VII				XIII
			E - Describe application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)			VII				XIII
			E - Describe application and system vulnerabilities and threats -- server-based			VII				XIII
			E - Describe application and system vulnerabilities and threats -- mainframe			VII				XIII
			E - Describe application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)			VII				XIII
C. General Awareness, Training and Education (AT&E)										
		1. Awareness, Training and Education (AT&E)								
			*E - Describe attack actions as training issues			V.d				
			E - Identify sources of AT&E materials			V.d				
D. General Countermeasures and Safeguards										
		2. AT&E								
			*E - Recognize awareness, training, and education (AT&E) as a countermeasure			V.d				
		3. Backup								
			*E - Define backup critical information			III,IX,XI				I,XV
		4. COMSEC								
			*E - Identify national COMSEC manager (Custodian)			X				
			E - Identify organizational COMSEC manager (Custodian)			X				
			E - List national COMSEC policies			XI				XVIII
			E - List national COMSEC procedures			XI				XVIII
		5. Countermeasures								
			*E - Describe what is meant by countermeasures			VIII				
		6. Digest								
			*E - Define message digests (i.e., MD5, SHA, HMAC)			IX				VII
		7. Digital Signature								
			*E - Define digital signatures			IX				VII
		8. Due Care								
			*E - Define due care (due diligence)			V				
		9. E-Mail								
			*E - Describe e-mail privacy countermeasures			IV-V				
			E - Describe e-mail privacy safeguards			IV-V				
		10. EMSEC/TEMPEST								
			*E - Define EMSEC/TEMPEST security countermeasures					III.h		
			E - Define EMSEC/TEMPEST security safeguards					III.h		
		11. Facilities								
			*E - Define facility support systems (i.e., fire protection and HVAC)			III-V				
		12. Hardware								
			*E - Define computing and telecommunications hardware/software	I.f						
		13. Internet								
			*E - Define internet security	I.g						
		14. Key								
			*E - Define key creation/distribution							VIII
			E - Define key recovery							VIII
			E - Define key storage/destruction							VIII
			E - Define PKI (Public Key Infrastructure) requirements							VIII
			E - Submit requirements for key management within the system							VIII
		15. Legal								
			*E - Define legal requirements			IV,XI			X	
		16. Marking								
			*E - Define marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media			IV,XI				
		17. Media								
			*E - Define magnetic media degaussing			IV,XI				
			E - Define marking, handling, storing, and destroying of sensitive information & media			IV,XI				
			E - Define media (i.e., tape, paper or disks) management			IV,XI				
			E - Define secure data deletion for media reuse			IV,XI				
		18. Misuse								
			*E - Define resource misuse prevention			IV,XI				

19. Non-Repudiation								
*E - Define digital non-repudiation			IV,XI				IX	
20. Operations								
*E - Describe information operations			I				I	
21. Privacy								
*E - Define privacy and protection			I				IX	
22. Privilege								
*E - Define need-to-know/least privilege							X	
E - Define operator/administrator privileges							X	
23. Record								
*E - Define record retention			IV,XI					
24. Safeguards								
*E - Define safeguards used to prevent software piracy			IV,XI					
E - Describe what is meant by safeguards			IV,XI					
25. Separation of Duties								
*E - Describe separation of duties as a countermeasure							X	
E - Explain separation of duties as a countermeasure							X	
26. Software Countermeasure								
*E - Define anti-virus systems	I.g		VIII				XIII	
E - Define countermeasures used to prevent software piracy						IV, IX		
27. Testing								
*E - Identify automated tools for security testing			IV					
28. Tools								
*E - Describe automated tools for security compliance			IV				XIV	
E - Describe automated tools for security test			IV				XIV	
E. Administrative Countermeasures/Safeguards								
1. Alarm								
*E - Describe alarms, signals and reports							XIV.e	
E - Identify alarms, signals and reports							XIV.e	
E - Implement alarms, signals and reports							XIV.e	
2. Assessment								
*E - Assist in preparing assessments			VI.e					
E - Prepare assessments for use during certification of information systems			VI.e					
3. System Test and Evaluation (ST&E)								
*E - Discuss System Test and Evaluation (ST&E) Plan and Procedures							XVIII	
E - Recommend revisions to System Test and Evaluation (ST&E) Plan and Procedures							XVIII	
4. Audit								
*E - Identify audit collection requirements							XII	
5. Certification								
*E - Discuss certification tools			VI.e					
E - Identify certification tools			VI.e					
E - Recommend use of specific certification tools			VI.e					
6. Control								
*E - Define application development control							XVI	
E - Define system software controls							XVI	
E - Differentiate security-related changes from non-security-related changes							XVI	
E - Identify storage media protection and control							XVI	
7. Countermeasures								
*E - Identify countermeasures			VIII					
12. Password								
*E - Address password management with staff			V					
E - Identify password management systems			V					
E - Define password management			V					
14. Recovery								
*E - Address recovery procedures with staff			III					
E - Describe disaster recovery procedures			III					
16. Separation of Duties								
*E - Define separation of duties							X	
E - Evaluate separation of duties							X	
E - Implement separation of duties							X	
F. Operations Policies/Procedures								
1. Assessment								
*E - Support assessments for use during certification of information systems			VI.e					
2. Countermeasures								
*E - Identify protective technologies			VIII					
E - List protective technologies			VIII					
3. Crime								
*E - Support anti-criminal activity preparedness planning (law enforcement)			III-IV					
5. Disposition								
*E - Identify disposition of media and data policies and procedures			IV					
6. Documentation								
*E - Describe documentation policy and procedures			II-IV					
7. Media								
*E - Identify storage media control policies and procedures			IV					
E - Identify storage media protection policies and procedures			IV					
9. Privacy								
*E - Outline known means of keystroke monitoring	I.g		IX					
10. Recovery								
*E - Define disaster recovery policies and procedures			III					
E - Describe disaster recovery policies and procedures			III					
11. Separation of Duties								
*E - Describe separation of duties policies and procedures							X	
12. Vendor								
*E - Facilitate vendor cooperation			II					
E - Explain vendor cooperation			II					

G. Contingency/Continuity of Operations								
	1. Backup							
		*E - Outline security policy for backup procedures		III				
	3. Continuity/Contingency							
		*E - Describe continuity/contingency planning		III				
		E - Prepare input to continuity/contingency plan		III				
	4. Recovery							
		*E - Describe disaster recovery		III				
		E - Describe disaster recovery plan testing		III				
		E - Prepare input to recovery plan		III				
FUNCTION 2 - INCIDENTS								
A. Policy and Procedures								
	2. Disposition							
		*E - Address disposition procedures with staff		III-IV				
	3. Due Care							
		*E - Address questions from users about due care		III-IV				
	4. Incident							
		*E - Define incidents		III-IV				
		E - Define breaches		III-IV				
		E - Address unauthorized access incident reporting with staff		III-IV				
		E - Define incident response		III-IV				
	5. Intrusion							
		*E - Define intrusion detection		VII-VIII				XIII
		E - Address intrusion detection management with staff		VII-VIII				XIII
	6. Legal							
		*E - Assist appropriate authority in witness interviewing/interrogation		III-V				
		E - Assist in evidence identification/preservation		III-V				
	7. Reporting							
		*E - Define reporting		V				
	9. Violation							
		*E - Define violations		V				
B. Operations Countermeasures/Safeguard								
	2. Attack							
		*E - Identify an attack		III				
	4. Authentication							
		*E - Address work force about authentication procedures		III				
	5. Organizational/Agency Systems Emergency Response Team							
		*E - Describe the organizational/agency systems emergency/incident response team		III				
	6. Countermeasure							
		*E - Assist in performing countermeasure/safeguard corrective actions		III				
		E - Describe countermeasures		III				
	7. Incident							
		*E - Address unauthorized access incident reporting with staff		III				
		E - Assist in incident response		III				
	9. Legal							
		*E - Assist appropriate authority in witness interviewing/interrogation		III-IV				
	10. Safeguard							
		*E - Describe safeguards		III				
C. Contingency Countermeasures/Safeguards								
	2. Availability							
		*E - Define information availability		I				
	3. Correction							
		*E - Identify examples of corrective actions		III				
	5. Incident							
		*E - Address unauthorized access incident reporting with staff		III				
	6. Intrusion							
		*E - Identify methods of intrusion detection		VIII				XIII
FUNCTION 3 - CONFIGURATION								
A. Administrative Policies/Procedures								
	3. Authentication							
		*E - Address authentication with staff		V				
		E - Address work force about authentication procedures		V				
	4. Biometrics							
		*E - Address biometric access management with staff		V				
	5. Organizational/Agency Systems Emergency/Incident Response Team							
		*E - Identify organizational/agency systems emergency/incident response team		V				
	6. Configure							
		*E - Define change control policies		V				
		E - Define configuration control		V				
		E - Address configuration management with staff		V				
		E - Address staff about legal configuration restrictions		V				
		E - Adhere to configuration control		V				
		E - Monitor configuration control		V				
	7. Copyright							
		*E - Adhere to copyright protection and licensing		V				
		E - Define copyright protection and licensing		V			IV	
	10. Install/Patch							
		*E - Identify appropriate sources for updates and patches		V				
	12. Management							
		*E - Identify basic/generic management issues		V	II.b			
	15. Operation							
		*E - Define operational procedure review		V				
	16. Password							
		*E - Address password management with staff		V				

FUNCTION 4 - ANOMALIES AND INTEGRITY								
A. General Risk Management								
	1. Attack							
		*E - Describe attack actions		VII-VIII				
		E - Identify attack actions		VII-VIII				
	3. EMSEC/TEMPEST							
		*E - Define EMSEC/TEMPEST security as it relates to the risk management process		VII-VIII		III.h		
		E - Describe EMSEC/TEMPEST security as it relates to the risk management process		VII-VIII		III.h		
	4. Internet							
		*E - Describe ways to provide protection for Internet connections		IX				XVII
	5. Legal							
		*E -Assist in investigations as requested		IV-V				
	6. Logging							
		*E - Describe the different categories of activities which may be logged		XI				XII
	7. Network							
		*E - Describe wireless security		IX				XIV
		E - Describe LAN/WAN security		IX				XIV
	8. Operating System							
		*E - Describe operating system integrity						XV-XVI
	10. Threat							
		*E - Identify different types of threat		I				I
	11. Zone							
		*E - Describe on what zoning and zone of control ratings are based						XV.g
B. Access Control Safeguards								
	1. Access Control							
		*E - Address access control software management with staff		IX				XI
		E - Address work force about access control software management procedures		IX				XI
		E - Define decentralized/distributed -- single sign on (SSO) (i.e., Kerberos)		IX				XI
		E - Define discretionary access controls		IX				XI
		E - Define mandatory access controls		IX				XI
		E - Define security domain		IX				XI
		E - Describe access control physical, logical, and administrative configurations		IX				XI
		E - Describe access rights and permissions		IX				XI
		E - Describe control techniques and policies (i.e., discretionary, mandatory, and rule of least privilege		IX				XI
		E - Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)		IX				XI
	2. Alarms							
		*E - Demonstrate the ability to use alarms, signals, and reports		IX				XIV.e
	3. Authentication							
		*E - Describe centralized/remote authentication access controls						IX
		E - Describe identification and authentication techniques						IX
		E - Identify identification and authentication techniques						IX
	4. Distribution System							
		*E - Define protected distribution systems						XVI
	6. Legal							
		*E - Address staff about legal access restrictions		XI				
		E - Assist in investigations as requested		XI				
	7. Monitor							
		*E - Define accountability and monitoring (i.e., correction, alarms, audit trail)		XI				
		E - Describe accountability and monitoring (i.e., correction, alarms, audit trail)		XI				
	8. Network							
		*E - Identify network security software		IX				XIV
	9. Operating System							
		*E - Describe operating system security features						XV-XVI
	10. Ownership							
		*E - Describe data ownership and custodianship		I				I
	11. Safeguards							
		*E - Describe system security safeguards		IX				XVI
C. Audit Policies and Procedures								
	1. Address							
		*E - Address access management with staff		V				
	4. Legal							
		*E - Address staff about legal access restrictions		V,XI				
		E - Assist in investigations as requested		V,XI				
	6. Separation of Duties							
		*E - Describe situations in which separation of duties is appropriate or mandatory		X				X
D. Audit Countermeasures/Safeguards								
	2. Legal							
		*E - Assist in investigations as requested		V,XI				
E. Audit Tools								
	1. Audit							
		*E - Define an error/audit log						XII
		E - Identify audit tools						XII
		E - Describe the major benefit gained through use of audit trails and logging policies						XII
	2. Intrusion							
		*E - Identify intrusion detection systems						XIII
	3. Legal							
		*E - Assist in investigations as requested		XI				
	4. Operating Systems							
		*E - Describe major operating system security features						XVI
F. Operations Management/Oversight								
	3. Configuration Management							
		*E - Describe configuration management		V				
	5. Legal							
		*E - Assist in investigations as requested		V,XI				

		6. Monitoring								
			*E - Address monitoring management with staff		V					
		8. Recovery								
			*E - Describe disaster recovery management		III,V					
			E - Describe disaster recovery oversight		III,V					
	G. Configuration Management									
		5. Legal								
			*E - Assist in investigations as requested		V					
		6. Media								
			*E - Identify storage media protection and control procedures		V					
		7. Subjects and Objects								
			*E - Define subjects and objects							III-VI
		10. Trusted Computer Base (TCB)								
			*E - Define trusted computer base (TCB) reference monitors and kernels							III-VI
FUNCTION 5 - ADMINISTRATION										
	A. Access Control Policies/Administration									
		1. Access Control								
			*E - Address access control software management with staff		V					
			E - Address access management with staff		V					
			E - Address work force about access control software management procedures		V					
			E - Address work force about access management procedures		V					
			E - Address work force about account management procedures		V					
			E - Describe data access		V					
		2. Accounts								
			*E - Address account management with staff		V					
		3. Authentication								
			*E - Address authentication with staff		V					
			E - Address work force about authentication procedures		V					
		5. Biometrics								
			*E - Address biometric access management with staff		V					
		7. Custodian								
			*E - Identify information resource custodian		V					
		8. Disposition								
			*E - Address disposition procedures with staff		V					
		9. Due Care								
			*E - Address questions from users about due care		V					
		10. Legal								
			*E - Address staff about legal access restrictions		V,XI					
			E - Address staff about legal monitoring restrictions		V,XI					
		11. Mode of Operation								
			*E - Define modes of operation		IV-V					XV
			E - Describe modes of operation		IV-V					XV
			E - Identify the dedicated mode of operation		IV-V					XV
		12. Monitoring								
			*E - Outline known means of electronic monitoring		III					XII
		13. Owner								
			*E - Identify information resource owner		I					I
			E - Define information ownership		I					I
		14. Password								
			*E - Describe a method to force regular password changes and the limitations of the method		IX					IX
		15. Separation of Duties								
			*E - Describe separation of duties							X
		16. Vendors								
			*E - Facilitate vendor cooperation		II,V					
		17. Audit								
			*E - Address work force about auditing and logging management procedures							XII
	B. Access Control Countermeasures									
		2. Authentication								
			*E - Address work force about authentication procedures		V					
		3. Biometrics								
			*E - Address biometric access management with staff		V					
		4. COMSEC Policy								
			*E - List national COMSEC policies		XI					XVIII
			E - List national COMSEC procedures		XI					XVIII
		5. Control								
			*E - Define internal controls and security		IV-V					
		6. Countermeasures								
			*E - Describe countermeasures		VIII					
			E - Define countermeasures		VIII					
			E - Give examples of countermeasures		VIII					
		8. Intrusion								
			*E - Identify methods of intrusion detection							XIII
			E - Address intrusion detection management with staff		V.d					XIII
			E - Address staff about intrusion detection		V.d					XIII
			E - Address staff about intrusion deterrents		V.d					XIII
		9. Isolation and Mediation								
			*E - Define isolation and mediation							XIV.e
		10. Key								
			*E - Demonstrate knowledge of how to operate a KMI-enabled system							VIII
			E - Submit requirements key management							VIII
		11. Monitoring								
			*E - Address monitoring management with staff		V.d					
			E - Address staff about monitoring and auditing intrusion detection policies		V.d					
			E - Address work force about monitoring management procedures		V.d					

		12. Network											
			*E - Define network firewalls						IX				XIV
			E - Describe network security software						IX				XIV
		13. Password											
			*E - Address password management with staff						V.d				
	C. Access Control Mechanisms												
		1. Access Control											
			*E - Define discretionary access controls										III,XI
			E - Define mandatory access controls										III,XI
			E - Describe discretionary access controls										III,XI
			E - Describe mandatory access controls										III,XI
		4. Biometrics											
			*E - Describe biometrics										IX.c
		9. Password											
			*E - Define one-time passwords										IX.a
			E - Define single sign-on										IX.a
			E - Describe one-time passwords										IX.a