

ANNE ARUNDEL COMMUNITY COLLEGE - CNSS 4013 MAPPING MATRIX				CSI 214	CSI 270	CSI 165
<b>FUNCTION 1 - SECURE USE</b>						
<b>A. General Security Policy</b>						
1.*Accountability						
		*E - Define organizational accountability policies		11.1	2.6	
		E - Outline accountability process/program		11.1	2.6	
2. Accreditation						
		*E - Define accreditation			4.9	
3. Architecture						
		*E - Define system security architecture			4	
		E - Identify appropriate security architecture for use in assigned IS			4	
		E - Address system security architecture study			4	
4. Assessment						
		*E - Define assessments for use during certification of information systems			4.9	
5. Assurance						
		*E - Define assurance			4.4	
6. Availability/Integrity/Confidentiality/Authentication/Non-repudiation						
		*E - Define concepts of availability, integrity, confidentiality, authentication, and non-repudiation		1.4	2.4/2.5	
7. Certification						
		*E - Define certification policies as related to organizational requirements			4.9	
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			4.8	
9. Configuration Control						
		*E - Define configuration control (management)			10.9/11.1.1.3.1	
10. Custodian						
		*E - Define resource custodian			2.2/2.11	
		E - Identify information resource custodian			2.2/2.11	
11. Defense in Depth						
		*E - Define defense in depth		L.O. I		
		E - Give examples of defense in depth methods		L.O. I		
		E - Give examples of defense in depth policy		L.O. I		
12. Document						
		*E - Identify DoDD 8500.1 policies (or appropriate civil agency guidance)		6.6	9.12	
13. Domains						
		*E - Define security domains as applicable to organizational policies			2.6	
		E - Describe security domains as applicable to organizational policies			2.6	
14. E-Mail						

		*E - Define organizational e-mail privacy policies			11.3/9.11	
15. Wireless Security						
		*E - Identify organizational wireless security policy			6.12	8
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			3.10.3	
		E - Describe EMSEC/TEMPEST control policies			3.10.3	
		E - Identify EMSEC/TEMPEST control policies			3.10.3	
		E - Identify EMSEC/TEMPEST security policies			3.10.3	
18. FAX						
		*E - Describe relevant FAX security policies			11.4	
19. Generally Accepted Security Principles						
		*E - Define generally accepted systems security principles	1.11		10/10.9	
20. Goals/Mission/Objectives						
		*E - Define goals, mission, and objectives of the organization			2.6	
21. Incident Response						
		*E - Describe incident response policies		7.3		
22. Information Assurance						
		*E - Define organizational Information Assurance (IA) policies			2.6/2.9	
23. Information Operations [DOD Organizations Only]						
		*E - Define information operations		11.0/11.1	2.1	
		E - Describe information operations		11.0/11.1	2.1	
		E - Support information operations		11.0/11.1	2.1	
24. Internet Security						
		*E - Describe organizational policies relevant to Internet security			6/6.10/7.13	
25. Law Enforcement						
		*E - Identify law enforcement interfaces			9.9	
		E - Describe law enforcement interfaces			9.9	
26. Marking						
		*E - Define policies relating to marking of classified, unclassified and sensitive information			2.10	
27. Monitoring						
		*E - Comply with legal aspects of monitoring			3.11	17.4
		E - Ensure legal aspects of monitoring are enforced			3.11	17.4
28. Multi-Level Security						
		*E - Describe multiple secure levels			4.4	
		E - Identify fundamental concepts of multilevel security			4.4	
		E - Define fundamental concepts of multilevel security			4.4	
		E - Describe fundamental concepts of multilevel security			4.4	
29. Network						
		*E - Describe computer network defense	8		6/6.4	13.3
		E - Describe policies relevant to network security			6	
		E - Describe wide area network (WAN) security policies			6.10	
30. Operating System						

		*E - Define functional requirements for operating system integrity			4.1.1	13.1
<b>32. Ownership</b>						
		*E - Define information ownership of data held under his/her cognizance			2.2/2.11	
		E - Identify information ownership of data held under his/her cognizance			2.2/2.11	
		E - Identify information resource owner			2.2/2.11	
<b>33. Physical Security</b>						
		*E - Define physical security		9	5.1	15
<b>34. Records Management</b>						
		*E - Define records management			2.1/2.2	
		E - Describe organizational security policies relative to electronic records management			2.1/2.2	
<b>37. Security Tools</b>						
		*E - Define automated security tools				L.O.b,c,d
<b>38. Sensitivity</b>						
		*E - Define information sensitivity			2.10	
		E - Describe information sensitivity in relation to organizational policies			2.10	
		E - Explain information sensitivity			2.10	
<b>39. Separation of Duties</b>						
		*E - Define separation of duties		11.6	11.1.1.1	
		E - Explain separation of duties		11.6	11.1.1.1	
		E - Define organizational policies relating to separation of duties		11.6	11.1.1.1	
<b>40. System Security</b>						
		*E - Identify systems security standards policies		6.1	10.9	
<b>41. Information Technology Security Evaluation Criteria (ITSEC)</b>						
		*E- Identify Information Security Technology Security Evaluation Criteria (ITSEC) policies			4.7	
<b>42. Testing</b>						
		*E - Define testing policies			10.9	
<b>43. Validation/Verification</b>						
		*E - Define validation policies			10.9	
		E - Identify verification and validation process policies			10.9	
<b>44. Workstation</b>						
		*E - Describe workstation security policies			6.4	9.9
<b>45. Zone</b>						
		*E - Define zone of control				11
		E - Define zoning				11
		E - Describe zoning and zone of control policies				11
<b>B. General Procedures</b>						
<b>1. Network Software</b>						
		*E - Define transport control protocol/internet protocol (TCP/IP)			6.2	4.7
		E - Define transport layer security (i.e., secure socket layer [SSL])			6.1	6.1
		E - Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)			6.11	4.5

		E - Define virtual private network (VPN) (i.e., SSH2, SOCKS)		p539	6.11	4.2
		E - Describe secure e-mail (i.e., PGP, S/MIME)			11.3	5/5.2
		E - Describe secure systems operations procedures			6	
		E - Describe transport control protocol/internet protocol (TCP/IP)			6.2	4.7
		E - Describe transport layer security (i.e., secure socket layer [SSL])			6.1	6.1
		E - Describe tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)		p539	6.11	4.5
		E - Describe virtual private network (VPN) (i.e., SSH2, SOCKS)			6.11	4.2
<b>2. Aggregation</b>						
		*E - Define aggregation			10.8.3	
		E - Describe aggregation			10.8.3	
<b>3. Application Vulnerabilities</b>						
		*E - Describe application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)			10/6.8	6
		E - Describe application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)			6.4/10	9.9
		E - Describe application and system vulnerabilities and threats -- server-based			6.4/10	9.9
		E - Describe application and system vulnerabilities and threats -- mainframe			6./10	L.O. c,d
		E - Describe application and system vulnerabilities and threats -- malicious code (i.e., Trojan horses, trap doors, viruses, worms)		p875	10.10	3
<b>4. Architecture</b>						
		*E - Address system security architecture study			4	
<b>5. Assessment</b>						
		*E - Prepare assessments for use during certification of information systems			4.9	
<b>7. Organizational/Agency Systems Emergency Response Team</b>						
		*E - Identify organizational/agency systems emergency response team		7.3		
		E - Report security issues to organizational/agency systems emergency response team		7.3		
<b>8. Database</b>						
		*E - Define data mining			10.8.4	
		E - Define databases and data warehousing vulnerabilities, threats and protections			10.8.4	
		E - Describe data mining			10.8.4	
		E - Describe databases and data warehousing vulnerabilities, threats and protections			10.8.4	
<b>9. EMSEC/TEMPEST</b>						
		*E - Define EMSEC/TEMPEST security procedures			3.10.3	
		E - Identify certified EMSEC/TEMPEST technical authority (CTTA)			3.10.3	
		E - Identify EMSEC/TEMPEST security procedures			3.10.3	
<b>10. End Systems</b>						
		*E - Define end systems (i.e., workstations, notebooks, PDA [personal digital assistant], smartphones, etc.)			6.12/6.4	9.9/9.10
		E - Describe end systems (i.e., workstations, notebooks, PDA, smartphones, etc.)			6.12/6.4	9.9/9.10
<b>11. Facility Management</b>						
		E - Practice facility management procedures		9	5	

12. FAX						
		*E - Practice facility management procedures		9	5	
		*E - Describe FAX security policies/procedures			11.4	p920
		E - Practice FAX security policies/procedures			11.4	
13. Housekeeping						
		*E - Define housekeeping procedures		11.1		
		E - Describe housekeeping procedures		11.1		
		E - Perform housekeeping procedures		11.1		
14. Inference						
		*E - Define Inference		10.8	4.3	
		E - Describe Inference		10.8	4.3	
15. Information States						
		*E - Define information states procedures(storage, transmission, processing)		1.5		
		E - Describe information states procedures		1.5		
16. Internet						
		*E - Define Internet security procedures			6.10	6
17. Investigations						
		*E - Assist in investigations as requested		3	9.9	
18. IPSEC						
		*E - Define IPSEC authentication and confidentiality			3.2/3.3	4.7
		E - Describe IPSEC authentication and confidentiality			3.2/3.3	4.7
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			2.10/2.10.2	
20. Multi-Level Security						
		*E - Define multilevel security			4.4	
21. Network, General						
		*E - Define network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)			6.4/6.4.1	
		E - Define network components (hardware, firmware, software, and media)			6.4/6.6	
		E - Define network layer security			6.1	
		E - Define network protocols			6.7	
		E - Define network types			6/6.4	
		E - Define wireless security			6.12	8
		E - Describe network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)			6.4/6.4.1	
		E - Describe network components (hardware, firmware, software, and media)			6.4/6.6	
		E - Describe network layer security			6.1	
		E - Describe network protocols			6.7	
		E - Describe network types			6/6.4	
		E - Describe WAN security procedures			6.10	
		E - Describe wireless security			6.12	8

		E - Discuss network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)			6.4/6.4.1	
		E - Practice WAN security procedures			6.10	
22. Network Hardware						
		*E - Define cable characteristics (i.e., twisted pair, fiber)			6.6	10.1
		E - Define concentrators			6.6	
		E - Define front-end processors, hubs, modems, multiplexers			6.6	
		E - Define gateways and routers			6.6	
		E - Define patch panels			6.6	
		E - Define routers			6.6	
		E - Define switches			6.6	
		E - Describe cable characteristics (i.e., twisted pair, fiber)			6.6	10.1
		E - Describe concentrators			6.6	
		E - Describe front-end processors, hubs, modems, multiplexers			6.6	
		E - Describe gateways and routers			6.6	
		E - Describe patch panels			6.6	
		E - Describe routers			6.6	
		E - Describe switches			6.6	
		E - Identify gateways and routers			6.6	
23. Network Software						
		*E - Define firewall architecture (i.e., bastion host, DMZ)		8.2		9.1
		E - Define firewall technology (i.e., packet filtering, data inspection)		8.2		9.1
		E - Define secure e-mail (i.e., PGP, S/MIME)				5/5.2
		E - Describe firewall architecture (i.e., bastion host, DMZ)		8.2		9.1
		E - Describe firewall technology (i.e., packet filtering, data inspection)		8.2		9.1
		E - Describe secure e-mail (i.e., PGP, S/MIME)				5/5.2
		E - Identify firewall architecture (i.e., bastion host, DMZ)		8.2		9.1
		E - Identify firewall technology (i.e., packet filtering, data inspection)		8.2		9.1
		E - Identify secure e-mail (i.e., PGP, S/MIME)				5/5.2
24. Objects						
		*E - Define object reuse			3.10.1	
		E - Define polyinstantiation			10.10 (p887)	
		E - Describe object reuse			3.10.1	
		E - Describe polyinstantiation			10.10 (p887)	
25. Operating System						
		*E - Define operating systems security procedures			4.1.1	13.1
		E - Describe operating system integrity procedures			4.1.1	13.1
		E - Perform operating systems security procedures			4.1.1	13.1
26. OSI (Open Systems Interconnect)						
		*E - Define application layer security protocols (i.e., secure electronic transactions, [personal digital assistant], smartphones, etc.)			6.1	
		E - Define data link layer security			6.1	
		E - Define network layer security			6.1	
		E - Define OSI model			6.1	

		E - Define transport control protocol/ internet protocol (TCP/IP)			6.1	
		E - Define transport layer security (i.e., secure socket layer [SSL])			6.1	
		E - Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)			6.1	
		E - Describe application layer security protocols (i.e., secure electronic transactions, secure hypertext, secure remote procedure call)			6.1	
		E - Describe data link layer security			6.1	
		E - Describe network layer security			6.1	
		E - Describe OSI model			6.1	
		E - Describe presentation layer			6.1	
		E - Describe session layer			6.1	
		E - Describe physical layer			6.1	
		E - Describe transport control protocol/ internet protocol (TCP/IP)			6.1	
		E - Describe transport layer security (i.e., secure socket layer [SSL])			6.1	
27. Rainbow Series						
		*E - Describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI) or Red Book as examples			4.6	
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			4.7	
					CH 5	
29. Security Procedures						
		*E - Define organizational security procedures		6.1	2.6	
		E - Assist in organizational security procedures		6.1	2.6	
30. Security tools						
		*E - Define automated security tools				13
		E - Describe automated security tools				13
31. Vulnerability and Threat						
		*E - Address application and system vulnerabilities and threats - mainframe			6	
		E - Address application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)			6.10	6
		E - Address application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)				9.9
		E - Address application and system vulnerabilities and threats -- server-based			6.6	9.9
		E - Address application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)				3
		E - Define application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)			6.10	6
		E - Define application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)				9.9
		E - Define application and system vulnerabilities and threats -- server-based			6.6	9.9
		E - Define application and system vulnerabilities and threats -- mainframe			6	
		E - Define application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)				3

	E - Describe application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)			6.10	6
	E - Describe application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)				9.9
	E - Describe application and system vulnerabilities and threats -- server-based			6.6	9.9
	E - Describe application and system vulnerabilities and threats -- mainframe			6	
	E - Describe application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)				3
<b>C. General Awareness, Training and Education (AT&amp;E)</b>					
1. Awareness, Training and Education (AT&E)					
	*E - Describe attack actions as training issues			6.9	17.3
	E - Identify sources of AT&E materials			6.9	17.3
<b>D. General Countermeasures and Safeguards</b>					
2. AT&E					
	*E - Recognize awareness, training, and education (AT&E) as a countermeasure			6.9	17.3
3. Backup					
	*E - Define backup critical information			8.2.4	
4. COMSEC					
	*E - Identify national COMSEC manager (Custodian)			2.2/2.11	
	E - Identify organizational COMSEC manager (Custodian)			2.2/2.11	
	E - List national COMSEC policies			6	7/9.12
	E - List national COMSEC procedures			6	7/9.12
5. Countermeasures					
	*E - Describe what is meant by countermeasures			2.8.6	
6. Digest					
	*E - Define message digests (i.e., MD5, SHA, HMAC)			7.8	
7. Digital Signature					
	*E - Define digital signatures			7.8	
8. Due Care					
	*E - Define due care (due diligence)			3.8	2.9 (p94)
9. E-Mail					
	*E - Describe e-mail privacy countermeasures			11.3	5
	E - Describe e-mail privacy safeguards			11.3	5
10. EMSEC/TEMPEST					
	*E - Define EMSEC/TEMPEST security countermeasures			3.10.3	
	E - Define EMSEC/TEMPEST security safeguards			3.10.3	
11. Facilities					
	*E - Define facility support systems (i.e., fire protection and HVAC)			9.2/9.3	5.4
12. Hardware					

		*E - Define computing and telecommunications hardware/software			6	
13. Internet						
		*E - Define internet security			6.10	6
14. Key						
		*E - Define key creation/distribution			3.4	14.5
		E - Define key recovery			3.4	14.5
		E - Define key storage/destruction			3.4	14.5
		E - Define PKI (Public Key Infrastructure) requirements			3.4	14.5
		E - Submit requirements for key management within the system			3.4	14.5
15. Legal						
		*E - Define legal requirements			9.12	
16. Marking						
		*E - Define marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media			2.10	
17. Media						
		*E - Define magnetic media degaussing			11.1.1.3.2	
		E - Define marking, handling, storing, and destroying of sensitive information & media			11.1.1.3.2	
		E - Define media (i.e., tape, paper or disks) management			11.1.1.3.2	
		E - Define secure data deletion for media reuse			11.1.1.3.2	
18. Misuse						
		*E - Define resource misuse prevention			2.7	
19. Non-Repudiation						
		*E - Define digital non-repudiation		App: Crypto	7.9	
20. Operations						
		*E - Describe information operations			2.1	
21. Privacy						
		*E - Define privacy and protection			9.11	
22. Privilege						
		*E - Define need-to-know/least privilege		11.6	11.1.1.1	
		E - Define operator/administrator privileges		11.6	11.1.1.1	
23. Record						
		*E - Define record retention			2.1/2.2.1	
24. Safeguards						
		*E - Define safeguards used to prevent software piracy		2.1	9.8 (p776)	
		E - Describe what is meant by safeguards			2.50	
25. Separation of Duties						
		*E - Describe separation of duties as a countermeasure			11.1.1.1	
		E - Explain separation of duties as a countermeasure			11.1.1.1	
26. Software Countermeasure						
		*E - Define anti-virus systems				3
		E - Define countermeasures used to prevent software piracy		2.1	9.8	p776
27. Testing						
		*E - Identify automated tools for security testing		8		3./6./11

28. Tools						
		*E - Describe automated tools for security compliance		8		3./6./11
		E - Describe automated tools for security test		8		3./6./11
<b>E. Administrative Countermeasures/Safeguards</b>						
1. Alarm						
		*E - Describe alarms, signals and reports		9.1	5	
		E - Identify alarms, signals and reports		9.1	5	
		E - Implement alarms, signals and reports		9.1	5	
2. Assessment						
		*E - Assist in preparing assessments			4.5/4.9	
		E - Prepare assessments for use during certification of information systems			4.5/4.9	
3. System Test and Evaluation (ST&E)						
		*E - Discuss System Test and Evaluation (ST&E) Plan and Procedures			4.5	
		E - Recommend revisions to System Test and Evaluation (ST&E) Plan and Procedures			4.5	
4. Audit						
		*E - Identify audit collection requirements			3.9/3.9.1	
5. Certification						
		*E - Discuss certification tools			4.9	
		E - Identify certification tools			4.9	
		E - Recommend use of specific certification tools			4.9	
6. Control						
		*E - Define application development control			10	
		E - Define system software controls				13.1/13.5
		E - Differentiate security-related changes from non-security-related changes			11.1.1.3	
		E - Identify storage media protection and control			11.1.1.3.2	10.6
7. Countermeasures						
		*E - Identify countermeasures			2.8/2.8.6	
12. Password						
		*E - Address password management with staff			3.3.3	
		E - Identify password management systems			3.3.3	
		E - Define password management			3.3.3	
14. Recovery						
		*E - Address recovery procedures with staff		7.7	8.1	16
		E - Describe disaster recovery procedures		7.7	8.1	16
16. Separation of Duties						
		*E - Define separation of duties			11.1.1.1	
		E - Evaluate separation of duties			11.1.1.1	
		E - Implement separation of duties			11.1.1.1	
<b>F. Operations Policies/Procedures</b>						

1. Assessment						
		*E - Support assessments for use during certification of information systems			4.9	
2. Countermeasures						
		*E - Identify protective technologies		8		13
		E - List protective technologies		8		13
3. Crime						
		*E - Support anti-criminal activity preparedness planning (law enforcement)		3	9.9	
5. Disposition						
		*E - Identify disposition of media and data policies and procedures			2.10	10.6
6. Documentation						
		*E - Describe documentation policy and procedures		1.11	10.9	
7. Media						
		*E - Identify storage media control policies and procedures			11.1.1.3.2	10.3/10.6
		E - Identify storage media protection policies and procedures			11.1.1.3.2	10.3/10.6
9. Privacy						
		*E - Outline known means of keystroke monitoring			3.9.2	
10. Recovery						
		*E - Define disaster recovery policies and procedures		7.7	8.1	16
		E - Describe disaster recovery policies and procedures		7.7	8.1	16
11. Separation of Duties						
		*E - Describe separation of duties policies and procedures		11.6	11.1.1.1	
12. Vendor						
		*E - Facilitate vendor cooperation			2.2/2.11	
		E - Explain vendor cooperation			2.1/2.11	
<b>G. Contingency/Continuity of Operations</b>						
1. Backup						
		*E - Outline security policy for backup procedures		7.7	8.2.4	
3. Continuity/Contingency						
		*E - Describe continuity/contingency planning		7	8	
		E - Prepare input to continuity/contingency plan		7	8	
4. Recovery						
		*E - Describe disaster recovery		7.7	8	
		E - Describe disaster recovery plan testing		7.7	8	
		E - Prepare input to recovery plan		7.7	8	
<b>FUNCTION 2 - INCIDENTS</b>						
<b>A. Policy and Procedures</b>						
2. Disposition						
		*E - Address disposition procedures with staff			2.10	

3. Due Care						
		*E - Address questions from users about due care		3.8	2.9 (p94)	
4. Incident						
		*E - Define incidents		7.3		12.5
		E - Define breaches		7.3		12.5
		E - Address unauthorized access incident reporting with staff		7.3		12.5
		E - Define incident response		7.3		12.5
5. Intrusion						
		*E - Define intrusion detection			3.13/5.5	12
		E - Address intrusion detection management with staff			3.13/5.5	12
6. Legal						
		*E - Assist appropriate authority in witness interviewing/interrogation			9.9	
		E - Assist in evidence identification/preservation			9.9	
7. Reporting						
		*E - Define reporting		7.3		12.5
9. Violation						
		*E - Define violations		7.3		12.5
<b>B. Operations Countermeasures/Safeguard</b>						
2. Attack						
		*E - Identify an attack		2.3		3
4. Authentication						
		*E - Address work force about authentication procedures			3.3	2
5. Organizational/Agency Systems Emergency Response Team						
		*E - Describe the organizational/agency systems emergency/incident response team		7.3		12.5
6. Countermeasure						
		*E - Assist in performing countermeasure/safeguard corrective actions		5.2	2.8.6	13
		E - Describe countermeasures		5.2	2.8.6	13
7. Incident						
		*E - Address unauthorized access incident reporting with staff		7.3		12.5
		E - Assist in incident response		7.3		12.5
9. Legal						
		*E - Assist appropriate authority in witness interviewing/interrogation			9.9	
10. Safeguard						
		*E - Describe safeguards			2.8.5	
<b>C. Contingency Countermeasures/Safeguards</b>						
2. Availability						
		*E - Define information availability		1.4	2.4.1	
3. Correction						
		*E - Identify examples of corrective actions			2.8	
5. Incident						

		*E - Address unauthorized access incident reporting with staff		7.3		12.5
<b>6. Intrusion</b>						
		*E - Identify methods of intrusion detection			3.13/5.5	12
<b>FUNCTION 3 - CONFIGURATION</b>						
<b>A. Administrative Policies/Procedures</b>						
<b>3. Authentication</b>						
		*E - Address authentication with staff			3.3	2
		E - Address work force about authentication procedures			3.3	2
<b>4. Biometrics</b>						
		*E - Address biometric access management with staff			3.3.2	
<b>5. Organizational/Agency Systems Emergency/Incident Response Team</b>						
		*E - Identify organizational/agency systems emergency/incident response team		7.3		12.5
<b>6. Configure</b>						
		*E - Define change control policies			11.1.1.3.1	
		E - Define configuration control			11.1.1.3.1	
		E - Address configuration management with staff			11.1.1.3.1	
		E - Address staff about legal configuration restrictions			11.1.1.3.1	
		E - Adhere to configuration control			11.1.1.3.1	
		E - Monitor configuration control			11.1.1.3.1	
<b>7. Copyright</b>						
		*E - Adhere to copyright protection and licensing			9.8	
		E - Define copyright protection and licensing			9.8	
<b>10. Install/Patch</b>						
		*E - Identify appropriate sources for updates and patches			10	13.1
<b>12. Management</b>						
		*E - Identify basic/generic management issues		12.2	2.1	
<b>15. Operation</b>						
		*E - Define operational procedure review			11	
<b>16. Password</b>						
		*E - Address password management with staff			3.3.3	
<b>FUNCTION 4 - ANOMALIES AND INTEGRITY</b>						
<b>A. General Risk Management</b>						
<b>1. Attack</b>						
		*E - Describe attack actions		2.3		3
		E - Identify attack actions		2.3		3

<b>3. EMSEC/TEMPEST</b>						
		*E - Define EMSEC/TEMPEST security as it relates to the risk management process			3.10.2/3.10.3	
		E - Describe EMSEC/TEMPEST security as it relates to the risk management process			3.10.2/3.10.3	
<b>4. Internet</b>						
		*E - Describe ways to provide protection for Internet connections			6.8	6
<b>5. Legal</b>						
		*E - Assist in investigations as requested			9.9	
<b>6. Logging</b>						
		*E - Describe the different categories of activities which may be logged			3.9	
<b>7. Network</b>						
		*E - Describe wireless security			6.12	8
		E - Describe LAN/WAN security			6.4/6.10	13.3
<b>8. Operating System</b>						
		*E - Describe operating system integrity			4.1.1	13/13.1
<b>10. Threat</b>						
		*E - Identify different types of threat		2.2		L.O. a
<b>11. Zone</b>						
		*E - Describe on what zoning and zone of control ratings are based				9, 11
<b>B. Access Control Safeguards</b>						
<b>1. Access Control</b>						
		*E - Address access control software management with staff			3	
		E - Address work force about access control software management procedures			3	
		E - Define decentralized/distributed -- single sign on (SSO) (i.e., Kerberos)			3	
		E - Define discretionary access controls			3	
		E - Define mandatory access controls			3	
		E - Define security domain			3	
		E - Describe access control physical, logical, and administrative configurations			3	
		E - Describe access rights and permissions			3	
		E - Describe control techniques and policies (i.e., discretionary, mandatory, and rule of least privilege)			3	
		E - Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)			3	
<b>2. Alarms</b>						
		*E - Demonstrate the ability to use alarms, signals, and reports			5	
<b>3. Authentication</b>						
		*E - Describe centralized/remote authentication access controls			3	
		E - Describe identification and authentication techniques			3	
		E - Identify identification and authentication techniques			3	
<b>4. Distribution System</b>						
		*E - Define protected distribution systems			10.10	

6. Legal						
		*E - Address staff about legal access restrictions			3	
		E - Assist in investigations as requested			9.9	
7. Monitor						
		*E - Define accountability and monitoring (i.e., correction, alarms, audit trail)			3.9	
		E - Describe accountability and monitoring (i.e., correction, alarms, audit trail)			3.9	
8. Network						
		*E - Identify network security software			6.4	13
9. Operating System						
		*E - Describe operating system security features			4.1.1	13.1
10. Ownership						
		*E - Describe data ownership and custodianship			2.11	
11. Safeguards						
		*E - Describe system security safeguards			10/10.9	
<b>C. Audit Policies and Procedures</b>						
1. Address						
		*E - Address access management with staff			3	
4. Legal						
		*E - Address staff about legal access restrictions			3	
		E - Assist in investigations as requested			9.9	
6. Separation of Duties						
		*E - Describe situations in which separation of duties is appropriate or mandatory		11.6	11.1.1.1	
<b>D. Audit Countermeasures/Safeguards</b>						
2. Legal						
		*E - Assist in investigations as requested			9.9	
<b>E. Audit Tools</b>						
1. Audit						
		*E - Define an error/audit log			3.9/3.9.1	
		E - Identify audit tools			3.9.1	
		E - Describe the major benefit gained through use of audit trails and logging policies			3.9.1	
2. Intrusion						
		*E - Identify intrusion detection systems			3.13/5.5	
3. Legal						
		*E - Assist in investigations as requested			9.9	
4. Operating Systems						
		*E - Describe major operating system security features			4.1.1	13.1
<b>F. Operations Management/Oversight</b>						

3. Configuration Management						
		*E - Describe configuration management			11.1.1.3.1	
5. Legal						
		*E - Assist in investigations as requested			9.9	
6. Monitoring						
		*E - Address monitoring management with staff			3	
8. Recovery						
		*E - Describe disaster recovery management		7.7	8.1	
		E - Describe disaster recovery oversight		7.7	8.1	
<b>G. Configuration Management</b>						
5. Legal						
		*E - Assist in investigations as requested			9.9	
6. Media						
		*E - Identify storage media protection and control procedures			11.1.1.3.2	10.3/10.6
7. Subjects and Objects						
		*E - Define subjects and objects			10.10	
10. Trusted Computer Base (TCB)						
		*E - Define trusted computer base (TCB) reference monitors and kernels			4.2.1	
<b>FUNCTION 5 - ADMINISTRATION</b>						
<b>A. Access Control Policies/Administration</b>						
1. Access Control						
		*E - Address access control software management with staff			3	
		E - Address access management with staff			3	
		E - Address work force about access control software management procedures			3	
		E - Address work force about access management procedures			3	
		E - Address work force about account management procedures			3	
		E - Describe data access			3	
2. Accounts						
		*E - Address account management with staff			3	
3. Authentication						
		*E - Address authentication with staff			3	2
		E - Address work force about authentication procedures			3	2
5. Biometrics						
		*E - Address biometric access management with staff			3.3.2	2.6
7. Custodian						
		*E - Identify information resource custodian			2.11/11.1.1	
8. Disposition						
		*E - Address disposition procedures with staff			2.10	

9. Due Care						
		*E - Address questions from users about due care		3.8	2.9 (p94)	
10. Legal						
		*E - Address staff about legal access restrictions			3	
		E - Address staff about legal monitoring restrictions			3.9	
11. Mode of Operation						
		*E - Define modes of operation			4.4	
		E - Describe modes of operation			4.4	
		E - Identify the dedicated mode of operation			4.4	
12. Monitoring						
		*E - Outline known means of electronic monitoring			5.3	
13. Owner						
		*E - Identify information resource owner			2.11/11.1.1	
		E - Define information ownership			2.11/11.1.1	
14. Password						
		*E - Describe a method to force regular password changes			3.3.3	
		and the limitations of the method				
15. Separation of Duties						
		*E - Describe separation of duties		11.6	11.1.1.1	
16. Vendors						
		*E - Facilitate vendor cooperation			2.2/2.11	
17. Audit						
		*E - Address work force about auditing and logging management procedures			3.9	
<b>B. Access Control Countermeasures</b>						
2. Authentication						
		*E - Address work force about authentication procedures			3.3	2
3. Biometrics						
		*E - Address biometric access management with staff			3.3.2	2.6
4. COMSEC Policy						
		*E - List national COMSEC policies		6	7	
		E - List national COMSEC procedures		6	7	
5. Control						
		*E - Define internal controls and security			2.9	
6. Countermeasures						
		*E - Describe countermeasures			2.8.6	
		E - Define countermeasures			2.8.6	
		E - Give examples of countermeasures			2.8.6	
8. Intrusion						
		*E - Identify methods of intrusion detection			3.13/5.5	12
		E - Address intrusion detection management with staff			3.13/5.5	12
		E - Address staff about intrusion detection			3.13/5.5	12
		E - Address staff about intrusion deterrents			3.13/5.5	12

9. Isolation and Mediation						
		*E - Define isolation and mediation			2.4/2.4.1	
10. Key						
		*E - Demonstrate knowledge of how to operate a KMI-enabled system			7.10	
		E - Submit requirements key management			7.10	
11. Monitoring						
		*E - Address monitoring management with staff			3.11	
		E - Address staff about monitoring and auditing intrusion detection policies			3.11/3.13	
		E - Address work force about monitoring management procedures			3.11	
12. Network						
		*E - Define network firewalls			6.6	9.1
		E - Describe network security software			6	
13. Password						
		*E - Address password management with staff			3.3.3	
<b>C. Access Control Mechanisms</b>						
1. Access Control						
		*E - Define discretionary access controls			3	
		E - Define mandatory access controls			3	
		E - Describe discretionary access controls			3	
		E - Describe mandatory access controls			3	
4. Biometrics						
		*E - Describe biometrics			3.3.2	
9. Password						
		*E - Define one-time passwords			3.3.3	
		E - Define single sign-on			3.3/3.4	
		E - Describe one-time passwords			3.3.3	