Table A.1. Rationale for Protections Countering Vulnerabilities

VULNERABILITIES/ATTACKS \ PROTECTIONS	A. Network connectivity protections	a. Authentication of network administrator	b. Robust network routing protocols	c. Dynamic routing	d. Firewalls, proxy services	e. VPN, Ipsec	f. QoS	g. Dynamic IP addressing	h. Mobile nodes	i. Survivable IP	j. Intelligent agents	B. Network management protections	a. Network monitoring	b. Service registration	c. SNMPv3	d. Robust and secure configuration and upgrading	e. Host and network IDS/IDR	C. Directory protections	a. DNSSEC	b. Dynamic DNS	c. Robust PKI	d. Directory-enabled networking protections	D. IDS and Cyber Panel vulnerability/attack protections	a. Protected control path	b. Robust IDS	E. Client/server/host protections	a. Strong authentication of user to end system	b. Authentication of client to network	c. Access control mechanisms	F. Software/firmware/middleware protections	a. Cryptographic checksums; "tripwire"	b. EAI protections	c. Spyware and exfiltration vulnerability/attack protections	d. End systems protections	e. Boundary protections	f. Covert channel vulnerability/attack protections	g. Covert channel detection methods	G. Personnel-related protections	a. Configuration management	b. Personnel controls	c. Internal system checks and protections
1. Network infrastructure vulnerabilities/attacks		X	X	X	X		X	X		X	X		X		X	X	X					X																	X	
a. Vulnerabilities of routers, switches, and similar network nodes		X	X	X			X	X		X	X		X		X	X	X					X																	X	
b. Vulnerabilities of boundary controllers, firewalls, proxies					X					X			X		X	X	X					X																	X	
c. Routing protocol attacks			X	X				X					X		X	X	X																						X	
d. Malicious protocol tunneling													X				X																						X	
e. Protocol misusage			X										X				X					X																	X	
f. Cause protocol changes			X			X							X			X	X																						X	
g. Attacks on links	X		X	X		X	X						X				X																						X	
h. Eavesdropping on network links						X											X																						X	
i. Network flooding			X	X			X			X			X				X																						X	
j. Cause links to go down	X	X	X	X			X						X				X																						X	
k. Network packet and data modification		X				X							X				X											X										X	
l. Spoofing attacks	X	X						X			X		X				X											X										X	
m. Man-in-the-middle attacks		X		X							X		X				X																					X	
n. Denial-of-service attacks on network	X					X					X		X				X																					X	
o. Distributed denial-of-service attacks on network	X				X	X					X		X				X																					X	
2. Directory vulnerabilities/attacks																		X	X	X	X	X																X	
a. Modify contents of directory																		X	X		X	X																X	
b. Denial-of-service attacks against directory																		X				X																X	
3. Network management node vulnerabilities/attacks												X	X	X	X	X	X					X																X	
a. Take management control												X	X		X		X					X																X	
b. Denial-of-service attacks against management node								X				X	X				X																					X	
4. Network authentication server vulnerabilities/attacks		X																			X	X																X	
a. Modify contents of authentication server																					X	X																X	
b. Denial-of-service attacks against authentication server								X														X																X	
5. PKI vulnerabilities/attacks																					X	X																X	
a. Modify certification authorities, certificates																					X	X																X	
6. Network operations vulnerabilities/attacks		X	X	X									X				X					X																X	
a. Isolate operations center		X	X	X									X																										X	
7. IDS and Cyber Panel vulnerabilities/attacks		X											X				X				X	X																X	
8. Client/server/host-based vulnerabilities/attacks		X																							X	X	X	X										X	
a. Prevent authentication																									X			X										X	
b. Circumvent authentication																									X	X	X											X	
c. Prevent client/server access to network																									X	X												X	
d. Circumvent or defeat access control mechanisms																													X									X	
e. Denial-of-service attacks on clients/servers																									X			X										X	
f. Distributed denial-of-service attacks against servers													X				X								X													X	
g. Modify clients/servers																									X	X	X	X		X									X	
9. Software/firmware/middleware vulnerabilities/attacks																							X							X	X								X	
a. Viruses, worms, Trojan horse program vulnerabilities/attacks													X				X													X									X	

Table A.1. Rationale for Protections Countering Vulnerabilities

PROTECTIONS	A. Network connectivity protections	a. Authentication of network administrator	b. Robust network routing protocols	c. Dynamic routing	d. Firewalls, proxy services	e. VPN, Ipsec	f. QoS	g. Dynamic IP addressing	h. Mobile nodes	i. Survivable IP	j. Intelligent agents	B. Network management protections	a. Network monitoring	b. Service registration	c. SNMPv3	d. Robust and secure configuration and upgrading	e. Host and network IDS/IDR	C. Directory protections	a. DNSSEC	b. Dynamic DNS	c. Robust PKI	d. Directory-enabled networking protections	D. IDS and Cyber Panel vulnerability/attack protections	a. Protected control path	b. Robust IDS	E. Client/server/host protections	a. Strong authentication of user to end system	b. Authentication of client to network	c. Access control mechanisms	F. Software/firmware/middleware protections	a. Cryptographic checksums; "tripwire"	b. EAI protections	c. Spyware and exfiltration vulnerability/attack protections	d. End systems protections	e. Boundary protections	f. Covert channel vulnerability/attack protections	g. Covert channel detection methods	G. Personnel-related protections	a. Configuration management	b. Personnel controls	c. Internal system checks and protections
b. Mobile code vulnerabilities/attacks											X		X	X		X																								
c. Life-cycle attacks/compromised software															X															X							X	X	X	
d. Attacks during software maintenance and updates		X																																				X	
e. Spyware and exfiltration vulnerabilities/attacks																																X	X	X				X	
f. Covert channel vulnerabilities/attacks																																			X	X		X	
10. Personnel-related vulnerabilities/attacks																																					X	X	X	
a. Vulnerabilities/attacks during development																																					X	X	X	
b. Vulnerabilities/attacks during installation																																					X	X	X	
c. Vulnerabilities/attacks during maintenance																																					X	X	X	
d. Vulnerabilities/attacks during service retirement																																					X	X	X	
e. Insider vulnerabilities/attacks																																							X	
f. Social engineering																																							X	X