Appendix A Primary Controls

The Primary Controls shown in this table serve as a guideline in the absence of a tailored prioritization of controls established by the ISSE or ISSM. Priority Controls may be added or omitted from this list for IT based on its unique characteristics or risk concerns. In the absence of security engineering, these Primary Controls may be used for an initial authorization decisions when a full test of the IT cannot be performed, and represent minimal testing required to enter ISCM. ISSMs of P1, 2, or 3 IT entering ISCM should reference the appropriate Test/Validate column as a guide when developing the IT ISCM strategy. Once Primary controls are tested, enhancements of Primary Control (not shown) are assessed before moving to the Secondary controls.

Control	Name	Priority 1 Test/ Validate	Priority 2 Test/ Validate	Priority 3 Test/ Validate	C			I			A		
					L	M	H	L	M	H	L	M	H
AC-3	Access Enforcement	Quarterly / Annual	Semi Annual / Annual	Annual/ Annual	Consult CNSSI 1253 for applicability								
AC-4	Information Flow Enforcement	Quarterly / Annual	Semi Annual / Annual	Annual/ Annual									
AC-17	Remote Access	Quarterly / Annual	Semi Annual / Annual	Annual/ Annual									
AU-6	Audit Review, Analysis, and Reporting	Monthly/ Annual	Quarterly / Annual	Annual/ Annual									
CA-5	Plan Of Action And Milestones												
CM-6	Configuration Settings	Annual/ Annual	Annual/ Annual	Annual/ Annual									
CP-4	Contingency Plan Testing	Monthly/ Annual											
CP-9	Information System Backup												
CP-10	Information System Recovery and	Annual/ Annual											

Control	Name	Priority 1 Test/ Validate	Priority 2 Test/ Validate	Priority 3 Test/ Validate	C			I			A		
					L	M	H	L	M	H	L	M	H
	Reconstitution												
IA-7	Cryptographic Module Authentication												
IR-3	Incident Response Testing	Semi Annual/ Annual	Semi Annual/ Annual										
PE-2	Physical Access Authorizations	Annual/ Annual											
PE-3	Physical Access Control	Annual/ Annual											
PL-2	System security plan												
RA-5	Vulnerability Scanning	Quarterly / Annual	Quarterly / Annual	Quarterly / Annual									
SA-15	Development Process, Standards, and Tools												
SC-5	Denial of Service Protection												
SC-7	Boundary Protection												
SC-8	Transmission Confidentiality and Integrity	Semi Annual/ Annual	Annual/ Annual	Annual/ Annual									
SC-12	Cryptographic Key Establishment and Management	Semi Annual/ Annual	Annual/ Annual	Annual/ Annual									
SC-13	Cryptographic Protection	Semi Annual/ Annual	Annual/ Annual	Annual/ Annual									

Control	Name	Priority 1 Test/ Validate	Priority 2 Test/ Validate	Priority 3 Test/ Validate	C			I			A		
					L	M	H	L	M	H	L	M	H
SC-23	Session Authenticity												
SC-28	Protection of Information at Rest												
SC-38	Operations Security												
SC-40	Wireless Link Protection												
SC-41	Port and I/O Device Access												
SC-42	Sensor Capability and Data												
SI-2	Flaw Remediation												
SI-4	Information System Monitoring												
SI-5	Security Alerts, Advisories, and Directives												
SI-6	Security Function Verification												
SI-7	Software, Firmware, and Information Integrity	Monthly/ Annual	Quarterly / Annual										
SI-10	Information Input Validation	Annual/ Annual	Annual/ Annual										
SI-11	Error Handling												
SI-15	Information Output Filtering												

Control	Name	Priority 1 Test/ Validate	Priority 2 Test/ Validate	Priority 3 Test/ Validate	C			I			A		
					L	M	H	L	M	H	L	M	H
SI-16	Memory Protection												

Appendix B Secondary Controls

Control enhancements are not shown, but must be tested as Secondary Controls are tested.

Control	Name	C			I			A		
		L	M	H	L	M	H	L	M	H
AC-2	Account Management	Consult CNSSI 1253 for applicability								
AC-6	Least Privilege									
AC-7	Unsuccessful Logon Attempts									
AC-12	Session Termination									
AC-18	Wireless Access									
AC-19	Access Control For Mobile Devices									
AU-5	Response to Audit Processing Failures									
AU-9	Protection of Audit Information									
AU-10	Non-Repudiation									
AU-12	Audit Generation									
CA-3	System Interconnections									
CA-6	Security Authorization									
CA-9	Internal System Connections									
CM-2	Baseline Configuration									
CM-5	Access Restrictions For Change									
CM-7	Least Functionality									
CM-8	Information System Component Inventory									
CM-9	Configuration Management Plan									
CM-10	Software Usage Restrictions									
CM-11	User-Installed Software									
IA-2	Identification and Authentication (Organizational Users)									
IA-3	Device Identification and Authentication									
IA-5	Authenticator Management									
IR-4	Incident Handling									
IR-6	Incident Reporting									
IR-8	Incident Response Plan									
IR-9	Information Spillage Response									
MA-4	Nonlocal Maintenance									
MP-3	Media Marking									
PE-4	Access Control For Transmission Medium									
PE-6	Monitoring Physical Access									

Control	Name	C			I			A		
		L	M	H	L	M	H	L	M	H
SA-4	Acquisition Process									
SA-9	External Information System Services									
SA-12	Supply Chain Protection									
SA-17	Developer Security Architecture and Design									
SA-22	Unsupported System Components									
SC-2	Application Partitioning									
SC-4	Information In Shared Resources									
SC-10	Network Disconnect									
SC-15	Collaborative Computing Devices									
SC-17	Public Key Infrastructure Certificates									
SC-18	Mobile Code									
SC-20	Secure Name / Address Resolution Service (Authoritative Source)									
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)									
SC-24	Fail In Known State									
SI-3	Malicious Code Protection									
SI-12	Information Handling and Retention									