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	Priority	Priority		C				I		A		
		1 Test/ Validate	2 Test/ Validate	3 Test/ Validate	L	M]	Η	L	M	Н	L	M	Н
AC-3	Access Enforcement	Quarterly / Annual	Semi Annual / Annual	Annual/ Annual		nsu plica				I 12	253 1	or		
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	Configuratio n 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												

Reconstituti on IA-7 Cryptograph ic Module Authenticati on IR-3 Incident Response Testing Annual/ Access Authorizatio ns PE-2 Physical Access Authorizatio ns PA-5 Vulnerabilit y Scanning SA-15 Developmen 1 Process, Standards, and Tools SC-7 Boundary Protection SC-8 Transmissio s SC-12 Cryptograph ic Key Annual/ Ann	Control	Name	Priority	Priority	Priority		С			Ι			A	
Reconstituti on IA-7				2 Test/	3 Test/	L	M	H	L	M	Н	L	M	H
IA-7 Cryptograph ic Module Authenticati on IR-3 Incident Response Annual/ Testing Annual Annual PE-2 Physical Annual Access Annual Access Control PL-2 System security plan RA-5 Vulnerabilit y Scanning SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n SC-8 Transmissio n Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Scanial Key Scanial Annual Annual Annual Annual Annual Annual Annual Annual SC-13 Cryptograph ic Key Scanial Cryptograph ic Key Growth and Scanial Cryptograph ic Fortection Annual Annual Annual Annual ic Protection Annual Annual Annual Annual ic Protection Annual Annual Annual Annual Annual Annual ic Protection Annual Annual Annual Annual Annual Annual ic Protection Annual			Validate	Validate	Validate									
IA-7 Cryptograph ic Module Authentication IR-3 Incident Response Annual/ Annual/ Annual/ Annual/ Access Annual/ Access Annual A		Reconstituti												
ic Module Authenticati on IR-3 Incident Response Testing Annual/ Annual/ PE-2 Physical Access Authorizatio ns PE-3 Physical Access Control PL-2 System security plan RA-5 Vulnerabilit y Scanning SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n SC-8 Transmissio n Confidentiali ty and Integrity SC-12 Cryptograph ic Key Establishme nt and Management SC-13 Cryptograph ic Forection SC-13 Cryptograph ic Forection SC-14 Cryptograph ic Forection SC-15 Cryptograph ic Forection SC-16 Cryptograph ic Forection SC-17 Cryptograph ic Forection SC-18 Cryptograph ic Forection SC-19 Cryptograph ic Forection SC-10 Cryptograph ic Forection SC-10 Cryptograph ic Forection SC-11 Cryptograph ic Forection SC-12 Cryptograph ic Forection SC-13 Cryptograph ic Forection SC-14 Cryptograph ic Forection SC-15 Cryptograph ic Forection SC-16 Cryptograph ic Forection SC-17 Cryptograph ic Forection SC-18 Cryptograph ic Forection SC-19 Cryptograph ic Forection SC-10 Cryptograph ic Forection SC-11 Cryptograph ic Forection SC-12 Cryptograph ic Forection SC-13 Cryptograph ic Forection SC-14 Cryptograph ic Forection SC-15 Cryptograph ic Forection SC-16 Cryptograph ic Forection SC-17 Cryptograph ic Forection SC-18 Cryptograph ic Forection SC-19 Cryptograph ic Forection SC-10 Cryptograph ic Forection SC-1														
R-3 Incident Response Response Annual/ Annual Annual PE-2 Physical Access Authorizatio ns PE-3 Physical Access Control PL-2 System security plan RA-5 Vulnerability Scanning SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n SC-7 Boundary Protection SC-8 Transmissio n Nanual Annual Confidentiality and Integrity SC-12 Cryptograph ic Key Establishmen at and Management SC-13 Cryptograph ic Frotection SC-13 Cryptograph ic Frotection Sc-14 Cryptograph ic Frotection Annual ic Frotection SC-13 Cryptograph ic Frotection Annual Ann	IA-7													
IR-3 Incident Response Annual/ Annual/ Annual/ Access Authorizatio ns PE-2 Physical Annual Annual Access Authorizatio ns PE-3 Physical Annual Access Control PL-2 System security plan RA-5 Vulnerabilit y Scanning / Annual / Annual / Annual Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n n Annual (Confidentiali ty and Integrity SC-12 Cryptograph ic Key Establishme nt and Management SC-13 Cryptograph ic Protection SC-13 Cryptograph ic Frotection SC-13 Cryptograph ic Protection Sc-13 Cryptograph ic Protection Annual														
IR-3 Incident Response Annual/ Annual Annual Annual PE-2 Physical Access Authorization RS PE-3 Physical Access Control PL-2 System Security plan RA-5 Vulnerabilit Y Scanning SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmission n Annual ty and Integrity SC-12 Cryptograph ic Key Establishmen at and Management SC-13 Cryptograph ic Frotection SC-13 Cryptograph ic Key Establishmen at and Management SC-13 Cryptograph ic Frotection Semi Annual Ann														
Response Testing Annual	IR ₋ 3		Semi	Semi										
Testing Annual Annual PE-2 Physical Annual/ Access Authorizatio ns PE-3 Physical Annual/ Access Control PL-2 System security plan RA-5 Vulnerabilit y Scanning / Annual / Annual PTrocess, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual/ Confidentiali ty and Integrity and Integrity SC-12 Cryptograph ic Key Annual Annual Annual Establishme nt and Management SC-13 Cryptograph ic Protection Semi Annual/ Annual SC-13 Cryptograph Semi ic Protection Annual/ Annual Annual Annual ic Protection Annual/ Annual Annual Annual Annual ic Protection Annual/ Annual	IIC 3													
PE-2 Physical Access Authorizatio ns														
Access Authorizatio ns PE-3 Physical Access Annual Control PL-2 System security plan RA-5 Vulnerabilit y Scanning / Annual / Annual / Annual SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual / Annual / Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Establishme nt and Management SC-13 Cryptograph ic Protection SC-13 Cryptograph ic Protection Semi Annual Annual Annual Annual Semi Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual SC-13 Cryptograph ic Protection Annual/ Annual Annual Establishme nt and Management SC-13 Cryptograph ic Protection Annual/ Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual	PE-2	•												
PE-3		-												
PE-3 Physical Access Annual Access Control PL-2 System security plan RA-5 Vulnerabilit y Scanning / Annual / Annual SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual Annual (Confidentiali ty and Integrity) SC-12 Cryptograph ic Key Annual Annual (Stablishme nt and Management (SC-13) SC-13 Cryptograph ic Protection (SC-13) SC-14 Cryptograph ic Rysical Annual (Annual Annual Annual Annual Annual Annual Annual (Annual Annual Annual Annual Annual Annual Annual Annual Annual (Annual Annual An		Authorizatio												
Access Control PL-2 System security plan security plan y System y System security plan y System security plan y System y System security plan y System y Sy		ns												
Control PL-2 System security plan RA-5 Vulnerabilit y Scanning / Annual / Annual SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual / Establishme nt and Management SC-13 Cryptograph ic Ryptograph ic Protection Semi Annual /	PE-3	Physical	Annual/											
PL-2 System security plan RA-5 Vulnerabilit y Scanning		Access	Annual											
RA-5 Vulnerabilit y Scanning /Annual /Annual /Annual SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual /Annual		Control												
RA-5 Vulnerabilit y Scanning /Annual /Annual /Annual SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Establishme nt and Management SC-13 Cryptograph ic Protection Semi Annual A	PL-2	•												
SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual Annual Annual ty and Integrity SC-12 Cryptograph ic Key Annual Annual Establishme nt and Management SC-13 Cryptograph ic Protection Semi Annual		• •												
SA-15 Developmen t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio Semi Annual/ Annual ty and Integrity SC-12 Cryptograph ic Key Annual/ Establishme nt and Management SC-13 Cryptograph ic Protection Semi Annual/ Annual	RA-5		-	-	_									
t Process, Standards, and Tools SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual/ Confidentiali ty and Integrity SC-12 Cryptograph ic Key Annual/ Bstablishme nt and Management SC-13 Cryptograph ic Protection Semi Annual/	G A 15		/ Annual	/ Annual	/ Annual	-								
SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual/ Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Annual/ Annual Establishme nt and Management SC-13 Cryptograph ic Protection Annual/	SA-15	_												
SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual/ Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Annual/ Annual Stablishme nt and Management SC-13 Cryptograph Semi Annual/ Annual/ Annual Annual/ Annual														
SC-5 Denial of Service Protection SC-7 Boundary Protection SC-8 Transmissio n Annual/ Annual Annual Annual ty and Integrity SC-12 Cryptograph ic Key Annual/ Annual Annual Annual Annual Annual Annual Stablishme nt and Management SC-13 Cryptograph ic Protection Annual/ Annual		,												
SC-7 Boundary Protection SC-8 Transmissio Semi Annual/ Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Annual/ Annual Annual Establishme Annual Annual Management SC-13 Cryptograph Semi Annual	SC-5													
SC-7 Boundary Protection SC-8 Transmissio Semi Annual/ Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Annual/ Annual Establishme nt and Management SC-13 Cryptograph ic Protection SC-14 Cryptograph Annual/ Annual														
SC-7 Boundary Protection SC-8 Transmissio Semi Annual/ Annual Confidentiali ty and Integrity SC-12 Cryptograph ic Key Annual/ Annual Establishme nt and Management SC-13 Cryptograph ic Protection SC-14 Cryptograph Annual														
SC-8 Transmissio Semi Annual/ Annual/ Annual Confidentiali Annual ty and Integrity SC-12 Cryptograph Semi Annual/ Annual Annual Establishme Annual Annual Int and Management SC-13 Cryptograph Semi Annual/	SC-7													
n Confidentiali Annual Annual Lity and Integrity SC-12 Cryptograph ic Key Annual Annual Annual Annual Annual Annual SC-13 Cryptograph ic Protection Annual		•												
Confidentiali ty and ty and Integrity SC-12 Cryptograph ic Key Annual/ Annual Annual Annual Annual Establishme nt and Management SC-13 Cryptograph ic Protection Annual/ Annual Annual Annual Annual Annual Annual Annual Annual Annual Annual	SC-8	Transmissio	Semi	Annual/	Annual/									
ty and Integrity SC-12 Cryptograph Semi Annual/ Annual/ Annual Establishme nt and Management SC-13 Cryptograph Semi Annual/		n	Annual/	Annual	Annual									
SC-12 Cryptograph Semi Annual/ Annual/ Annual Establishme nt and Management SC-13 Cryptograph Semi Annual/ Ann			Annual											
SC-12 Cryptograph ic Key Annual/ Annual Annual Annual Annual Annual Establishme nt and Management SC-13 Cryptograph ic Protection Annual Annual Annual Annual Annual		-												
ic Key Annual Annual Annual Establishme Annual Annual Management SC-13 Cryptograph Semi Annual Annual Annual Annual Annual Annual														
Establishme nt and Management SC-13 Cryptograph Semi Annual/ Annual/ Annual Annual	SC-12													
nt and Management SC-13 Cryptograph Semi Annual/ Annual/ ic Protection Annual/ Annual Annual				Annual	Annual									
Management SC-13 Cryptograph Semi Annual/ Annual/ ic Protection Annual/ Annual Annual			Annual											
SC-13 Cryptograph Semi Annual/ Annual/ Annual/ Annual														
ic Protection Annual Annual Annual	SC-13		Semi	Annual/	Annual/	1								
	50 15	• • • •												
i i i i i i i i i i i i i i i i i i i		10 Trotteetion	Annual	1 minuui	1 minuu									

Control	Name	Priority	Priority	Priority		С			I			A		
	Tunit	1 Test/ Validate	2 Test/ Validate	3 Test/ Validate	L		Н	L	M	Н	L	M	Н	
SC-23	Session Authenticity	, 0220000	, C22C3C3C	, 0.220.000					ı					
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	Priority	Priority		C		I			A		
		1 Test/	2 Test/	3 Test/	L	M	H	L	M	H	L	\mathbf{M}	H
		Validate	Validate	Validate									
SI-16	Memory												
	Protection												

Appendix B Secondary Controls

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

Control	Name		С			I		A		
		L	M	Н	L	M	Н	L	M	Н
AC-2	Account Management	Co	nsult	t CN	ISSI	125	3 fo	r		
AC-6	Least Privilege	applicability								
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	7								
PE-4	Access Control For Transmission Medium									
PE-6	Monitoring Physical Access									

Control	Name		C		I				A	
		L	M	Н	L	M	Н	L	M	Н
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									