Draft ICS Requirement Baselines

Modifications to original SP 800-53 Baselines are in pink

REQ NO.	REQUIREMENT NAME	REQUIREMENT BASELINES		
		LOW	MOD	HIGH
Access Requirement				
AC-1	Access Requirement Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1) (2)	AC-3 (1) (2)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Requirement	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Requirement	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Requirement for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4

REQ NO.	REQUIREMENT NAME	REQUIREMENT BASELINES		
		LOW	MOD	HIGH
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6 (2)	AU-6 (1) (2)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
Certification, Accreditation, and Security Assessments				
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4 (1)	CA-4 (1)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
Configuration Management				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Requirement	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (2)
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	Not Selected	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)

REQ NO.	REQUIREMENT NAME	REQUIREMENT BASELINES		
		LOW	MOD	HIGH
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2	IA-2 (1)	IA-2 (2) (3)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4 (1) (2)	MA-4 (1) (2) ~~(3)~~
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	Not Selected	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1) (2)	MP-5 (1) (2) (3)
MP-6	Media Sanitization and Disposal	MP-6	MP-6	MP-6 (1) (2)
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Requirement	PE-3	PE-3	PE-3 (1)
PE-4	Access Requirement for Transmission Medium	Not Selected	Not Selected	PE-4
PE-5	Access Requirement for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)

REQ NO.	REQUIREMENT NAME	REQUIREMENT BASELINES		
		LOW	MOD	HIGH
PE-7	Visitor Requirement	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9 (1)	PE-9 (1) (2)
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10 (1)
PE-11	Emergency Power	Not Selected PE-11	PE-11 (1)	PE-11 (1) (2)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Requirements	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4 (1)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5 (1)
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Selected	RA-5	RA-5 (1) (2)

REQ NO.	REQUIREMENT NAME	REQUIREMENT BASELINES		
		LOW	MOD	HIGH
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8 (1)
SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information Remnance	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5)	SC-7 (1) (2) (3) (4) (5) (6)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address	Not Selected	SC-22	SC-22

REQ NO.	REQUIREMENT NAME	REQUIREMENT BASELINES		
		LOW	MOD	HIGH
	Resolution Service			
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring Tools and Techniques	Not Selected	SI-4 (4)	SI-4 (2) (4) (5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7 (1) (2)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12