

Recommended Security Controls for Federal Information Systems and Organizations

Note: CNTL NO. Table D2: Security Control Base Lines (Derived From Appendix F)

Minimum Requirements: FedRamp Security Controls Version 1.1

Security Control Name		Low-Impact	Medium-Impact	Comments
<b>Access Control Family</b>				
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	
AC-5	Separation of Duties	Not Selected	AC-5	
<b>Awareness and Training Control Family</b>				
AT-4	Security Training Records	AT-4	AT-4	
<b>Security Assessment and Authorization Control Family</b>				
CA-2	Security Assessments	CA-2	CA-2 (1)	
CA-3	Information System Connections	CA-3	CA-3	
CA-5	Plan of Action and Milestones	CA-5	CA-5	
<b>Configuration Management Control Family</b>				
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3) (4) ? delete (4) @ Rev 4	
CM-6	Configuration Settings	CM-6	CM-6 (3)	
CM-9	Configuration Management Plan	Not Selected	CM-9	Developed by vendor for ATO
<b>Contingency Planning Control Family</b>				
CP-2	Contingency Plan	CP-2	CP-2 (1) ? add (3) (8) @ Rev 4	Developed by vendor for ATO
CP-4	Contingency Plan Testing and Exercises	CP-4	CP-4 (1)	
<b>Identification and Authentication Control Family</b>				
IA-5	Authenticator Management	IA-5 (1)	IA-5 (1) (2) (3)	
<b>Incident Response Control Family</b>				
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3 ? add (2) @ Rev 4	
<b>Maintenance Control Family</b>				
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	
<b>Physical and Environmental Protection Control Family</b>				
PE-2	Physical Access Authorizations	PE-2	PE-2	
PE-8	Access Records	PE-8	PE-8	
<b>Planning Control Family</b>				
PL-2	System Security Plan	PL-2	PL-2 ? add (3) @ Rev 4	Developed by vendor for ATO
PL-4	Rules of Behavior	PL-4	PL-4 ? add (1) @ Rev 4	
PL-5	Privacy Impact Assessment	PL-5	PL-5 ? Withdrawn @ Rev 4	Required if PII data is being provided to vendor
<b>Personnel Security Control Family</b>				
PS-7	Third-Party Personnel Security	PS-7	PS-7 ? add (1) @ Rev 4	
<b>Risk Assessment Control Family</b>				
RA-5	Vulnerability Scanning	RA-5	RA-5 (1)	
<b>System and Communications Protection Control Family</b>				
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5) (7)	
<b>System and Information Integrity Control Family</b>				
SI-2	Flaw Remediation	SI-2	SI-2 (2)	
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2) (3)	

Notes: