NIST 800-53 WORKSHEET

Instructions: please complete the “Contractor Implemented” column. Acceptable answers are “yes”, “no”, “shared control”, and “N/A.”

#	CNTL NO.	CONTROL NAME	Pri	FISMA Low	FISMA Mod	Service Provider Implemented?
1	AC-1	Access Control Policy and Procedures	P1	Y	Y	
2	AC-2	Account Management	P1	Y	Y	
3	AC-3	Access Enforcement	P1	Y	Y	
4	AC-4	Information Flow Enforcement	P1	N	Y	
5	AC-5	Separation of Duties	P1	N	Y	
6	AC-6	Least Privilege	P1	N	Y	
7	AC-7	Unsuccessful Logon Attempts	P2	Y	Y	
8	AC-8	System Use Notification	P1	Y	Y	
9	AC-11	Session Lock	P3	N	Y	
10	AC-12	Session Termination	P2	N	Y	
11	AC-14	Permitted Actions without Identification or Authentication	P3	Y	Y	
12	AC-17	Remote Access	P1	Y	Y	
13	AC-18	Wireless Access	P1	Y	Y	
14	AC-19	Access Control for Mobile Devices	P1	Y	Y	
15	AC-20	Use of External Information Systems	P1	Y	Y	
16	AC-21	Information Sharing	P2	N	Y	
17	AC-22	Publicly Accessible Content	P3	Y	Y	
18	AT-1	Security Awareness and Training Policy and Procedures	P1	Y	Y	
19	AT-2	Security Awareness Training	P1	Y	Y	
20	AT-3	Role-Based Security Training	P1	Y	Y	
21	AT-4	Security Training Records	P3	Y	Y	
22	AU-1	Audit and Accountability Policy and Procedures	P1	Y	Y	
23	AU-2	Audit Events	P1	Y	Y	
24	AU-3	Content of Audit Records	P1	Y	Y	
25	AU-4	Audit Storage Capacity	P1	Y	Y	
26	AU-5	Response to Audit Processing Failures	P1	Y	Y	
27	AU-6	Audit Review, Analysis, and Reporting	P1	Y	Y	
28	AU-7	Audit Reduction and Report Generation	P2	N	Y	
29	AU-8	Time Stamps	P1	Y	Y	
30	AU-9	Protection of Audit Information	P1	Y	Y	
31	AU-11	Audit Record Retention	P3	Y	Y	
32	AU-12	Audit Generation	P1	Y	Y	
33	CA-1	Security Assessment and Authorization Policies and Procedures	P1	Y	Y	
34	CA-2	Security Assessments	P2	Y	Y	
35	CA-3	System Interconnections	P1	Y	Y	
36	CA-5	Plan of Action and Milestones	P3	Y	Y	
37	CA-6	Security Authorization	P2	Y	Y	
38	CA-7	Continuous Monitoring	P2	Y	Y	
39	CA-9	Internal System Connections	P2	Y	Y	

NIST 800-53 WORKSHEET

Instructions: please complete the “Contractor Implemented” column. Acceptable answers are “yes”, “no”, “shared control”, and “N/A.”

40	CM-1	Configuration Management Policy and Procedures	P1	Y	Y	
41	CM-2	Baseline Configuration	P1	Y	Y	
42	CM-3	Configuration Change Control	P1	N	Y	
43	CM-4	Security Impact Analysis	P2	Y	Y	
44	CM-5	Access Restrictions for Change	P1	N	Y	
45	CM-6	Configuration Settings	P1	Y	Y	
46	CM-7	Least Functionality	P1	Y	Y	
47	CM-8	Information System Component Inventory	P1	Y	Y	
48	CM-9	Configuration Management Plan	P1	N	Y	
49	CM-10	Software Usage Restrictions	P2	Y	Y	
50	CM-11	User-Installed Software	P1	Y	Y	
51	CP-1	Contingency Planning Policy and Procedures	P1	Y	Y	
52	CP-2	Contingency Plan	P1	Y	Y	
53	CP-3	Contingency Training	P2	Y	Y	
54	CP-4	Contingency Plan Testing	P2	Y	Y	
55	CP-6	Alternate Storage Site	P1	N	Y	
56	CP-7	Alternate Processing Site	P1	N	Y	
57	CP-8	Telecommunications Services	P1	N	Y	
58	CP-9	Information System Backup	P1	Y	Y	
59	CP-10	Information System Recovery and Reconstitution	P1	Y	Y	
60	IA-1	Identification and Authentication Policy and Procedures	P1	Y	Y	
61	IA-2	Identification and Authentication (Organizational Users)	P1	Y	Y	
62	IA-3	Device Identification and Authentication	P1	N	Y	
63	IA-4	Identifier Management	P1	Y	Y	
64	IA-5	Authenticator Management	P1	Y	Y	
65	IA-6	Authenticator Feedback	P2	Y	Y	
66	IA-7	Cryptographic Module Authentication	P1	Y	Y	
67	IA-8	Identification and Authentication (Non-Organizational Users)	P1	Y	Y	
68	IR-1	Incident Response Policy and Procedures	P1	Y	Y	
69	IR-2	Incident Response Training	P2	Y	Y	
70	IR-3	Incident Response Testing	P2	N	Y	
71	IR-4	Incident Handling	P1	Y	Y	
72	IR-5	Incident Monitoring	P1	Y	Y	
73	IR-6	Incident Reporting	P1	Y	Y	
74	IR-7	Incident Response Assistance	P2	Y	Y	
75	IR-8	Incident Response Plan	P1	Y	Y	
76	MA-1	System Maintenance Policy and Procedures	P1	Y	Y	
77	MA-2	Controlled Maintenance	P2	Y	Y	
78	MA-3	Maintenance Tools	P3	N	Y	
79	MA-4	Nonlocal Maintenance	P2	Y	Y	

NIST 800-53 WORKSHEET

Instructions: please complete the “Contractor Implemented” column. Acceptable answers are “yes”, “no”, “shared control”, and “N/A.”

80	MA-5	Maintenance Personnel	P2	Y	Y	
81	MA-6	Timely Maintenance	P2	N	Y	
82	MP-1	Media Protection Policy and Procedures	P1	Y	Y	
83	MP-2	Media Access	P1	Y	Y	
84	MP-3	Media Marking	P2	N	Y	
85	MP-4	Media Storage	P1	N	Y	
86	MP-5	Media Transport	P1	N	Y	
87	MP-6	Media Sanitization	P1	Y	Y	
88	MP-7	Media Use	P1	Y	Y	
89	PE-1	Physical and Environmental Protection Policy and Procedures	P1	Y	Y	
90	PE-2	Physical Access Authorizations	P1	Y	Y	
91	PE-3	Physical Access Control	P1	Y	Y	
92	PE-4	Access Control for Transmission Medium	P1	N	Y	
93	PE-5	Access Control for Output Devices	P2	N	Y	
94	PE-6	Monitoring Physical Access	P1	Y	Y	
95	PE-8	Visitor Access Records	P3	Y	Y	
96	PE-9	Power Equipment and Cabling	P1	N	Y	
97	PE-10	Emergency Shutoff	P1	N	Y	
98	PE-11	Emergency Power	P1	N	Y	
99	PE-12	Emergency Lighting	P1	Y	Y	
100	PE-13	Fire Protection	P1	Y	Y	
101	PE-14	Temperature and Humidity Controls	P1	Y	Y	
102	PE-15	Water Damage Protection	P1	Y	Y	
103	PE-16	Delivery and Removal	P2	Y	Y	
104	PE-17	Alternate Work Site	P2	N	Y	
105	PL-1	Security Planning Policy and Procedures	P1	Y	Y	
106	PL-2	System Security Plan	P1	Y	Y	
107	PL-4	Rules of Behavior	P2	Y	Y	
108	PL-8	Information Security Architecture	P1	N	Y	
109	PS-1	Personnel Security Policy and Procedures	P1	Y	Y	
110	PS-2	Position Risk Designation	P1	Y	Y	
111	PS-3	Personnel Screening	P1	Y	Y	
112	PS-4	Personnel Termination	P1	Y	Y	
113	PS-5	Personnel Transfer	P2	Y	Y	
114	PS-6	Access Agreements	P3	Y	Y	
115	PS-7	Third-Party Personnel Security	P1	Y	Y	
116	PS-8	Personnel Sanctions	P3	Y	Y	
117	RA-1	Risk Assessment Policy and Procedures	P1	Y	Y	
118	RA-2	Security Categorization	P1	Y	Y	
119	RA-3	Risk Assessment	P1	Y	Y	
120	RA-5	Vulnerability Scanning	P1	Y	Y	
121	SA-1	System and Services Acquisition Policy and Procedures	P1	Y	Y	
122	SA-2	Allocation of Resources	P1	Y	Y	

NIST 800-53 WORKSHEET

Instructions: please complete the “Contractor Implemented” column. Acceptable answers are “yes”, “no”, “shared control”, and “N/A.”

123	SA-3	System Development Life Cycle	P1	Y	Y	
124	SA-4	Acquisition Process	P1	Y	Y	
125	SA-5	Information System Documentation	P2	Y	Y	
126	SA-8	Security Engineering Principles	P1	N	Y	
127	SA-9	External Information System Services	P1	Y	Y	
128	SA-10	Developer Configuration Management	P1	N	Y	
129	SA-11	Developer Security Testing and Evaluation	P1	N	Y	
130	SC-1	System and Communications Protection Policy and Procedures	P1	Y	Y	
131	SC-2	Application Partitioning	P1	N	Y	
132	SC-4	Information in Shared Resources	P1	N	Y	
133	SC-5	Denial of Service Protection	P1	Y	Y	
134	SC-7	Boundary Protection	P1	Y	Y	
135	SC-8	Transmission Confidentiality and Integrity	P1	N	Y	
136	SC-10	Network Disconnect	P2	N	Y	
137	SC-12	Cryptographic Key Establishment and Management	P1	Y	Y	
138	SC-13	Cryptographic Protection	P1	Y	Y	
139	SC-15	Collaborative Computing Devices	P1	Y	Y	
140	SC-17	Public Key Infrastructure Certificates	P1	N	Y	
141	SC-18	Mobile Code	P2	N	Y	
142	SC-19	Voice Over Internet Protocol	P1	N	Y	
143	SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	Y	Y	
144	SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	Y	Y	
145	SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	Y	Y	
146	SC-23	Session Authenticity	P1	N	Y	
147	SC-28	Protection of Information at Rest	P1	N	Y	
148	SC-39	Process Isolation	P1	Y	Y	
149	SI-1	System and Information Integrity Policy and Procedures	P1	Y	Y	
150	SI-2	Flaw Remediation	P1	Y	Y	
151	SI-3	Malicious Code Protection	P1	Y	Y	
152	SI-4	Information System Monitoring	P1	Y	Y	
153	SI-5	Security Alerts, Advisories, and Directives	P1	Y	Y	
154	SI-7	Software, Firmware, and Information Integrity	P1	N	Y	
155	SI-8	Spam Protection	P2	N	Y	
156	SI-10	Information Input Validation	P1	N	Y	
157	SI-11	Error Handling	P2	N	Y	
158	SI-12	Information Handling and Retention	P2	Y	Y	
159	SI-16	Memory Protection	P1	N	Y	