NIST Special Publication 800-53 Revision 4

800-53 SECURITY CONTROLS

National Institute of Standards and Technology (NIST)

OVERVIEW

The catalog of security controls provides a range of safeguards and countermeasures for organizations and information systems. The security controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines. The security controls in the catalog with few exceptions, have been designed to be policy- and technology-neutral. This means that security controls and control enhancements focus on the fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission.

ABOUT NIST

Special Publication 800-53 is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act of 2002 (FISMA) and to help with managing cost effective programs to protect their information and information systems.

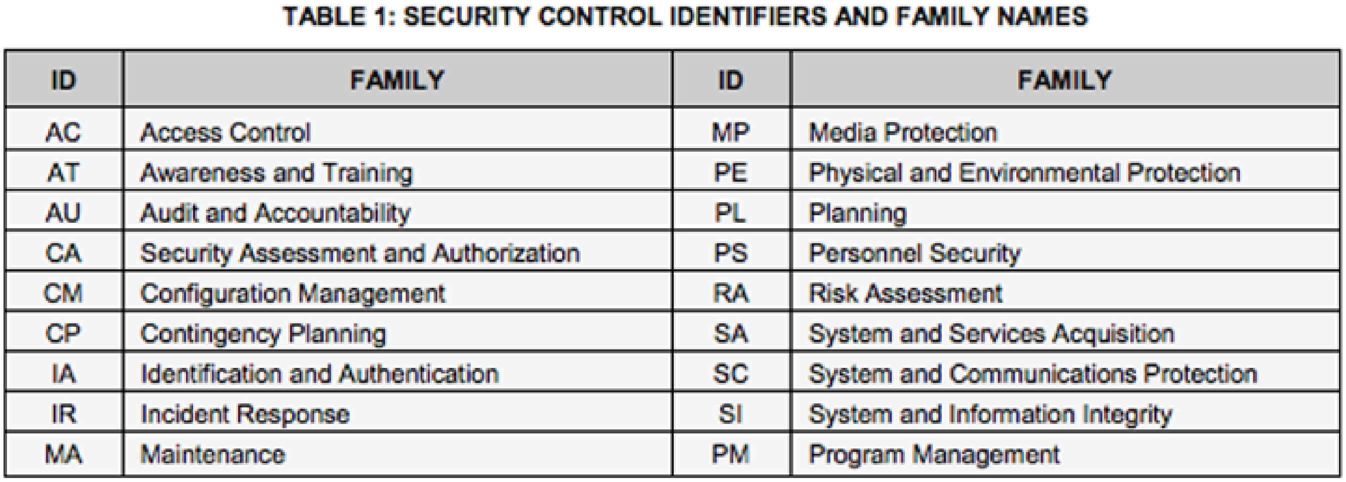

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

800-53 SECURITY CONTROLS

National Institute of Standards and Technology (NIST)

□ NIST Control Family 1: Access Control

- *AC-1 Access Control Policy and Procedures*
- *AC-2 Account Management*
- *AC-3 Access Enforcement*
- *AC-4 Information Flow Enforcement*
- *AC-5 Separation of Duties*
- *AC-6 Least Privilege*
- *AC-7 Unsuccessful Logon Attempts*
- *AC-8 System Use Notification*
- *AC-9 Previous Logon (Access) Notification*
- *AC-10 Concurrent Session Control*
- *AC-11 Session Lock*
- *AC-12 Session Termination*
- *AC-13 Withdrawn*
- *AC-14 Permitted Actions w/o Identification orAuthentication*
- *AC-15 Withdrawn*
- *AC-16 Security Attributes*
- *AC-17 Remote Access*
- *AC-18 Wireless Access*
- *AC-19 Access Control for Mobile Devices*
- *AC-20 Use of External Information Systems*
- *AC-21 Information Sharing*
- *AC-22 Publicly Accessible Content*
- *AC-23 Data Mining Protection*
- *AC-24 Access Control Decisions*
- *AC-25 Reference Monitor*

□ NIST Control Family 2: Awareness and Training

- *AT-1 Security Awareness and Training Policy and Procedures*
- *AT-2 Security Awareness Training*
- *AT-3 Role-Based Security Training*
- *AT-4 Security Training Records*
- *AT-5 Withdrawn*

□ NIST Control Family 3: Audit and Accountability

- *AU-1 Audit and Accountability Policy and Procedures*
- *AU-2 Audit Events*
- *AU-3 Content of Audit Records*
- *AU-4 Audit Storage Capacity*
- *AU-5 Response to Audit Processing Failures*
- *AU-6 Audit Review, Analysis, and Reporting*
- *AU-7 Audit Reduction and Report Generation*
- *AU-8 Time Stamps*
- *AU-9 Protection of Audit Information*
- *AU-10 Non-repudiation*
- *AU-11 Audit Record Retention*
- *AU-12 Audit Generation*
- *AU-13 Monitoring for Information Disclosure*
- *AU-14 Session Audit*
- *AU-15 Alternate Audit Capability*
- *AU-16 Cross-Organizational Auditing*

□ NIST Control Family 4: Security Assessment and Authorization

- *CA-1 Security Assessment/Authorization Policies/Procedures*
- *CA-2 Security Assessments*
- *CA-3 System Interconnections*
- *CA-4 Withdrawn*
- *CA-5 Plan of Action and Milestones*
- *CA-6 Security Authorization*
- *CA-7 Continuous Monitoring*
- *CA-8 Penetration Testing*
- *CA-9 Internal System Connections*

800-53 SECURITY CONTROLS

National Institute of Standards and Technology (NIST)

□ NIST Control Family 5: Configuration Management

- *CM-1 Configuration Management Policy and Procedures*
- *CM-2 Baseline Configuration*
- *CM-3 Configuration Change Control*
- *CM-4 Security Impact Analysis*
- *CM-5 Access Restrictions for Change*
- *CM-6 Configuration Settings*
- *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*

□ NIST Control Family 6: Contingency Planning

- *CP-1 Contingency Planning Policy and Procedures*
- *CP-2 Contingency Plan*
- *CP-3 Contingency Training*
- *CP-4 Contingency Plan Testing*
- *CP-5 Withdrawn*
- *CP-6 Alternate Storage Site*
- *CP-7 Alternate Processing Site*
- *CP-8 Telecommunications Services*
- *CP-9 Information System Backup*
- *CP-10 Information System Recovery/Reconstitution*
- *CP-11 Alternate Communications Protocols*
- *CP-12 Safe Mode*
- *CP-13 Alternative Security Mechanisms*

□ NIST Control Family 7: Identification and Authentication

- *IA-1 Identification and Authentication Policy and Procedures*
- *IA-2 Identification and Authentication (Organizational Users)*
- *IA-3 Device Identification and Authentication*
- *IA-4 Identifier Management*
- *IA-5 Authenticator Management*
- *IA-6 Authenticator Feedback*
- *IA-7 Cryptographic Module Authentication*
- *IA-8 Identification and Authentication*
- *IA-9 Service Identification and Authentication*
- *IA-10 Adaptive Identification and Authentication*
- *IA-11 Re-authentication*

□ NIST Control Family 8: Incident Response

- *IR-1 Incident Response Policy and Procedures*
- *IR-2 Incident Response Training*
- *IR-3 Incident Response Testing*
- *IR-4 Incident Handling*
- *IR-5 Incident Monitoring*
- *IR-6 Incident Reporting*
- *IR-7 Incident Response Assistance*
- *IR-8 Incident Response Plan*
- *IR-9 Information Spillage Response*
- *IR-10 Integrated Information Security Analysis*

800-53 SECURITY CONTROLS

National Institute of Standards and Technology (NIST)

□ NIST Control Family 9: Maintenance

- *MA-1 System Maintenance Policy and Procedures*
- *MA-2 Controlled Maintenance*
- *MA-3 Maintenance Tools*
- *MA-4 Nonlocal Maintenance*
- *MA-5 Maintenance Personnel*
- *MA-6 Timely Maintenance*

□ NIST Control Family 10: Media Protection

- *MP-1 Media Protection Policy and Procedures*
- *MP-2 Media Access*
- *MP-3 Media Marking*
- *MP-4 Media Storage*
- *MP-5 Media Transport*
- *MP-6 Media Sanitization*
- *MP-7 Media Use*
- *MP-8 Media Downgrading*

□ NIST Control Family 11: Physical and Environmental Protection

- *PE-1 Physical and Environmental Protection Policy and Procedures*
- *PE-2 Physical Access Authorizations*
- *PE-3 Physical Access Control*
- *PE-4 Access Control for Transmission Medium*
- *PE-5 Access Control for Output Devices*
- *PE-6 Monitoring Physical Access*
- *PE-7 Withdrawn*
- *PE-8 Visitor Access Records*
- *PE-9 Power Equipment and Cabling*
- *PE-10 Emergency Shutoff*
- *PE-11 Emergency Power*
- *PE-12 Emergency Lighting*
- *PE-13 Fire Protection*
- *PE-14 Temperature and Humidity Controls*
- *PE-15 Water Damage Protection*
- *PE-16 Delivery and Removal*
- *PE-17 Alternate Work Site*
- *PE-18 Location of Info. System Components*
- *PE-19 Information Leakage*
- *PE-20 Asset Monitoring and Tracking*

□ NIST Control Family 12: Planning

- *PL-1 Security Planning Policy and Procedures*
- *PL-2 System Security Plan*
- *PL-3 Withdrawn*
- *PL-4 Rules of Behavior*
- *PL-5 Withdrawn*
- *PL-6 Withdrawn*
- *PL-7 Security Concept of Operations*
- *PL-8 Information Security Architecture*
- *PL-9 Central Management*

□ NIST Control Family 13: Personnel Security

- *PS-1 Personnel Security Policy and Procedures*
- *PS-2 Position Risk Designation*
- *PS-3 Personnel Screening*
- *PS-4 Personnel Termination*
- *PS-5 Personnel Transfer*
- *PS-6 Access Agreements*
- *PS-7 Third-Party Personnel Security*
- *PS-8 Personnel Sanctions*

800-53 SECURITY CONTROLS

National Institute of Standards and Technology (NIST)

□ **NIST Control Family 14: Risk Assessment**

- *RA-1 Risk Assessment Policy and Procedures*
- *RA-2 Security Categorization*
- *RA-3 Risk Assessment*
- *RA-4 Withdrawn*
- *RA-5 Vulnerability Scanning*
- *RA-6 Technical Surveillance Countermeasures*

□ **NIST Control Family 15: System and Services Acquisition**

- *SA-1 System and Services Acquisition Policy and Procedures*
- *SA-2 Allocation of Resources*
- *SA-3 System Development Life Cycle*
- *SA-4 Acquisition Process*
- *SA-5 Information System Documentation*
- *SA-6 Withdrawn*
- *SA-7 Withdrawn*
- *SA-8 Security Engineering Principles*
- *SA-9 External Information System Services*
- *SA-10 Developer Configuration Management*
- *SA-11 Developer Security Testing and Evaluation*
- *SA-12 Supply Chain Protection*
- *SA-13 Trustworthiness*
- *SA-14 Criticality Analysis*
- *SA-15 Development Process, Standards, Tools*
- *SA-16 Developer-Provided Training*
- *SA-17 Developer Security Architecture/Design*
- *SA-18 Tamper Resistance and Detection*
- *SA-19 Component Authenticity*
- *SA-20 Cust. Development of Critical Components*
- *SA-21 Developer Screening*
- *SA-22 Unsupported System Components*

800-53 SECURITY CONTROLS

National Institute of Standards and Technology (NIST)

□ **NIST Control Family 16: System and Communications Protection**

- *SC-1 System/Communications Protection Policy/Procedures*
- *SC-2 Application Partitioning*
- *SC-3 Security Function Isolation*
- *SC-4 Information in Shared Resources*
- *SC-5 Denial of Service Protection*
- *SC-6 Resource Availability*
- *SC-7 Boundary Protection*
- *SC-8 Transmission Confidentiality and Integrity*
- *SC-10 Network Disconnect*
- *SC-11 Trusted Path*
- *SC-12 Cryptographic Key Establishment and Management*
- *SC-13 Cryptographic Protection*
- *SC-15 Collaborative Computing Devices*
- *SC-16 Transmission of Security Attributes*
- *SC-17 Public Key Infrastructure Certificates*
- *SC-18 Mobile Code*
- *SC-19 Voice Over Internet Protocol*
- *SC-20 Secure Name /Address Resolution Service*
- *SC-21 Secure Name /Address Resolution Service*
- *SC-22 Architecture and Provisioning*
- *SC-23 Session Authenticity*

SC-24 Fail in Known State
SC-25 Thin Nodes
SC-26 Honeypots
SC-27 Platform-Independent Applications
SC-28 Protection of Information at Rest
SC-29 Heterogeneity
SC-30 Concealment and Misdirection
SC-31 Covert Channel Analysis
SC-32 Information System Partitioning
SC-34 Non-Modifiable Executable Programs
SC-35 Honeyclients
SC-36 Distributed Processing and Storage
SC-37 Out-of-Band Channels
SC-38 Operations Security
SC-39 Process Isolation
SC-40 Wireless Link Protection
SC-41 Port and I/O Device Access
SC-42 Sensor Capability and Data
SC-43 Usage Restrictions
SC-44 Detonation Chambers

□ **NIST Control Family 17: System and Information Integrity**

- *SI-1 System and Information Integrity Policy and Procedures*

SI-2 Flaw Remediation
SI-3 Malicious Code Protection
SI-4 Information System Monitoring
SI-5 Security Alerts, Advisories, and Directives
SI-6 Security Function Verification
SI-7 Software, Firmware, and Information Integrity
SI-8 Spam Protection
SI-9 Withdrawn

SI-10 Information Input Validation
SI-11 Error Handling
SI-12 Information Handling and Retention
SI-13 Predictable Failure Prevention
SI-14 Non-Persistence
SI-15 Information Output Filtering
SI-16 Memory Protection
SI-17 Fail-Safe Procedures