Appendix A. Security Control Mappings

Relationship of Security Controls to Other Standards and Control Sets

The first mapping table in this appendix provides organizations a general indication of SP 800-53 security control coverage with respect to other frequently referenced security control standards and control sets.[1] The security control mappings are not exhaustive and are based on a broad interpretation and general understanding of the control sets being compared. The mappings are created by using the primary security topic identified in each of the SP 800-53 security controls and searching for a similar security topic in the other referenced security control standards and control sets. Security controls with similar functional meaning (e.g., SP 800-53, *Contingency Planning,* and ISO/International Electrotechnical Commission [IEC] 17799, *Business Continuity*) are included in the mapping table. In some instances, similar topics are addressed in the security control sets but provide a different context, perspective, or scope (e.g., SP 800-53 addresses privacy requirements in terms of privacy policy notification, whereas ISO/IEC 17799 addresses privacy requirements in terms of legislation and regulations). Organizations are encouraged to use the mapping table as a starting point for conducting further analysis and interpretation of control similarity and associated coverage when comparing disparate control sets.

1 The Security Control Mapping table includes references to: (i) NIST SP 800-53, *Contingency Planning*; (ii) ISO/IEC 17799:2000, *Code of Practice for Information Security Management*; (iii) NIST SP 800-26, *Security Self-Assessment Guide for Information Technology System*; and (iv) GAO, *Federal Information System Controls Audit Manual*. The numerical designations in the respective columns indicate the paragraph number(s) in the above documents where the security controls, control objectives, or associated implementation guidance may be found.

NIST 800-53 to HUD Information Technology Security Policy Mapping

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
Access Control				
5.2.1	AC-1	Access Control Policy and Procedures	11.1.1 11.4.1 15.1.1	---
5.2.2	AC-2	Account Management	6.2.2 6.2.3 8.3.3 11.2.1 11.2.2 11.2.4 11.7.2	AC-2.1 AC-2.2 AC-3.2 SP-4.1
5.2.3	AC-3	Access Enforcement	11.2.4 11.4.5	AC-2 AC-3.2
5.2.4	AC-4	Information Flow Enforcement	10.6.2 11.4.5 11.4.6 11.4.7	---
5.2.5	AC-5	Separation of Duties	10.1.3 10.6.1 10.10.1	AC-3.2 SD-1.2
5.2.6	AC-6	Least Privilege	11.2.2	AC-3.2
5.2.7	AC-7	Unsuccessful Login Attempts	11.5.1	AC-3.2
5.2.8	AC-8	System Use Notification	11.5.1 15.1.5	AC-3.2
5.2.9 (Optional Control)	AC-9	Previous Logon Notification	11.5.1	AC-3.2
5.2.10	AC-10	Concurrent Session Control	---	---
5.2.11	AC-11	Session Lock	11.3.2	AC-3.2
5.2.12	AC-12	Session Termination	11.3.2 11.5.5	AC-3.2
5.2.13	AC-13	Supervision and Review—Access Control	10.10.2 11.2.4	AC-4 AC-4.3 SS-2.2
5.2.14	AC-14	Permitted Actions without Identification or Authentication	---	---
5.2.15	AC-15	Automated Marking	7.2.2	AC-3.2
5.2.16 (Optional control)	AC-16	Automated Labeling	7.2.2	AC-3.2
5.2.17	AC-17	Remote Access	11.4.2 11.4.3 11.4.4	AC-3.2

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
5.2.18	AC-18	Wireless Access Restrictions	11.4.2 11.7.1 11.7.2	---
5.2.19	AC-19	Access Control for Portable and Mobile Devices	11.7.1	---
5.2.20	AC-20	Use of External Information Systems	6.1.4 9.2.5 11.7.1	---
5.2.21	--	HUD Policy Title – Person Use of Government Equipment	--	--
Awareness and Training				
4.9.1	AT-1	Security Awareness and Training Policy and Procedures	5.1.1 8.2.2 15.1.1	---
4.9.2	AT-2	Security Awareness	6.2.3 8.2.2 10.4.1 11.7.1 13.1.1 14.1.4 15.1.4	---
4.9.3	AT-3	Security Training	8.2.2 10.3.2 11.7.1 13.1.1 14.1.4	---
4.9.4	AT-4	Security Training Records	---	---
4.9.5	AT-5	Contacts with Security Groups and Associations	6.1.7	---
Audit and Accountability				
5.3.1	AU-1	Audit and Accountability Policy and Procedures	10.10 15.1.1	---
5.3.2	AU-2	Auditable Events	10.10.1	---
5.3.3	AU-3	Content of Audit Records	10.10.1 10.10.4	---
5.3.4	AU-4	Audit Storage Capacity	10.10.3	---
5.3.5	AU-5	Response to Audit Processing Failures	10.10.3	---
5.3.6	AU-6	Audit Monitoring, Analysis, and Reporting	10.10.2 10.10.4 13.2.1	AC-4.3
5.3.7	AU-7	Audit Reduction and Report Generation	10.10.3	---
5.3.8	AU-8	Time Stamps	10.10.6	---
5.3.9	AU-9	Protection of Audit Information	10.10.3 15.1.3 15.3.2	---
5.3.10	AU-10	Non-repudiation	10.8.2 10.9.1 12.3.1	---

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
5.3.11	AU-11	Audit Record Retention	10.10.1 15.1.3	---
Certification, Accreditation, and Security Assessments				
3.4.1	CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	6.1.4 10.3.2 15.1.1	---
3.4.2	CA-2	Security Assessments	6.1.8 15.2.1 15.2.2	SP-5.1
3.4.3	CA-3	Information System Connections	10.6.2 10.9.1 11.4.5 11.4.6 11.4.7	CC-2.1
3.4.4	CA-4	Security Certification	10.3.2	CC-2.1
3.4.5	CA-5	Plan of Action and Milestones	15.2.1	SP-5.1 SP-5.2
3.4.6	CA-6	Security Accreditation	10.3.2	---
3.4.7	CA-7	Continuous Monitoring	15.2.1 15.2.2	---
Configuration Management				
4.4.1	CM-1	Configuration Management Policy and Procedures	12.4.1 12.5.1 15.1.1	---
4.4.2	CM-2	Baseline Configuration	7.1.1 15.1.2	CC-2.3 CC-3.1 SS-1.2
4.4.3	CM-3	Configuration Change Control	10.1.2 10.2.3 12.4.1 12.5.1 12.5.2 12.5.3	SS-3.2 CC-2.2
4.4.4	CM-4	Monitoring Configuration Changes	10.1.2	SS-3.1 SS-3.2 CC-2.1
4.4.5	CM-5	Access Restrictions for Change	11.6.1	SD-1.1 SS-1.2 SS-2.1
4.4.6	CM-6	Configuration Settings	---	---
4.4.7	CM-7	Least Functionality	---	---

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
4.4.8	CM-8	Information System Component Inventory	7.1.1 15.1.2	CC-2.3 CC-3.1 SS-1.2
Contingency Planning				
4.3.1	CP-1	Contingency Planning Policy and Procedures	5.1.1 10.4.1 14.1.1 14.1.3 15.1.1	---
4.3.2	CP-2	Contingency Plan	10.3.2 10.4.1 10.8.5 14.1.3 14.1.4	SC-3.1 SC-1.1
4.3.3	CP-3	Contingency Training	14.1.3 14.1.4	SC-2.3
4.3.4	CP-4	Contingency Plan Testing and Exercises	10.5.1 14.1.5	SC-3.1
4.3.5	CP-5	Contingency Plan Update	14.1.3 14.1.5	SC-2.1 SC-3.1
4.3.6	CP-6	Alternate Storage Site	10.5.1	SC-2.1 SC-3.1
4.3.7	CP-7	Alternate Processing Site	14.1.4	SC-2.1 SC-3.1
4.3.8	CP-8	Telecommunications Services	14.1.4	---
4.3.9	CP-9	Information System Backup	10.5.1 11.7.1	SC-2.1
4.3.10	CP-10	Information System Recovery and Reconstitution	14.1.4	SC-2.1
Identification and Authentication				
5.1.1	IA-1	Identification and Authentication Policy and Procedures	15.1.1	---
5.1.2	IA-2	User Identification and Authentication	11.2.3 11.4.2 11.5.2	---
5.1.3	IA-3	Device Identification and Authentication	11.4.2 11.4.3 11.7.1	---
5.1.4	IA-4	Identifier Management	11.2.3 11.5.2	AC-2.1 AC-3.2 SP-4.1
5.1.5	IA-5	Authenticator Management	11.5.2 11.5.3	AC-3.2
5.1.6	IA-6	Authenticator Feedback	11.5.1	---
5.1.7	IA-7	Cryptographic Module Authentication	---	---

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
Incident Response				
4.8.1	IR-1	Incident Response Policy and Procedures	10.4.1 13.1 13.2.1 15.1.1	---
4.8.2	IR-2	Incident Response Training	13.1.1	SP-3.4
4.8.3	IR-3	Incident Response Testing and Exercises	14.1.5	---
4.8.4	IR-4	Incident Handling	6.1.6 13.2.1 13.2.2	SP-3.4
4.8.5	IR-5	Incident Monitoring	---	---
4.8.6	IR-6	Incident Reporting	6.1.6 6.2.2 6.2.3 13.1.1 13.1.2	---
4.8.7	IR-7	Incident Response Assistance	14.1.3	SP-3.4
Maintenance				
4.5.1	MA-1	System Maintenance Policy and Procedures	10.1.1 15.1.1	---
4.5.2	MA-2	Controlled Maintenance	9.2.4	SS-3.1
4.5.3	MA-3	Maintenance Tools	---	---
4.5.4	MA-4	Remote Maintenance	11.4.4	SS-3.1
4.5.5	MA-5	Maintenance Personnel	6.2.3 9.2.4	SS-3.1
4.5.6	MA-6	Timely Maintenance	---	SC-1.2
Media Protection				
4.7.1	MP-1	Media Protection Policy and Procedures	10.1.1 10.7 15.1.1 15.1.3	---
4.7.2	MP-2	Media Access	10.7.3	---
4.7.3	MP-3	Media Labeling	7.2.2 10.7.3 10.8.2 15.1.3	---
4.7.4	MP-4	Media Storage	10.7.1 10.7.2 10.7.3 10.7.4 15.1.3	AC-3.1
4.7.5	MP-5	Media Transport	10.8.3	---
4.7.6	MP-6	Media Sanitization and Disposal	9.2.6 10.7.1 10.7.2	AC-3.4
Physical and Environmental Protection				
4.2.1	PE-1	Physical and Environmental Protection Policy and Procedures	15.1.1	

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
4.2.2	PE-2	Physical Access Authorizations	9.1.2 9.1.6	AC-3.1
4.2.3	PE-3	Physical Access Control	9.1.1 9.1.2 9.1.5 9.1.6 10.5.1	AC-3.1
4.2.4	PE-4	Access Control for Transmission Medium	9.2.3	---
4.2.5	PE-5	Access Control for Display Medium	9.1.2 11.3.3	---
4.2.6	PE-6	Monitoring Physical Access	9.1.2	AC-4
4.2.7	PE-7	Visitor Control	9.1.2	AC-3.1
4.2.8	PE-8	Access Records	9.1.2	AC-4
4.2.9	PE-9	Power Equipment and Power Cabling	9.2.2 9.2.3	SC-2.2
4.2.10	PE-10	Emergency Shutoff	9.2.2	---
4.2.11	PE-11	Emergency Power	9.2.2	SC-2.2
4.2.12	PE-12	Emergency Lighting	9.2.2	---
4.2.13	PE-13	Fire Protection	9.1.4 9.2.1	SC-2.2
4.2.14	PE-14	Temperature and Humidity Controls	9.2.1 10.5.1 10.7.1	SC-2.2
4.2.15	PE-15	Water Damage Protection	9.1.4 9.2.1	SC-2.2
4.2.16	PE-16	Delivery and Removal	9.1.6 9.2.7 10.7.1	AC-3.1
4.2.17	PE-17	Alternate Work Site	11.7.2	---
4.2.18	PE-18	Location of Information System Components	9.2.1	---
4.2.19	PE-19	Information Leakage	---	---
4.2.20	---	HUD Policy Title – Facilities Housing HUD Information Systems	---	AC-3
4.2.21	---	HUD Policy Title – Redundant Air-Cooling Systems	---	---
Planning				
3.2.1	PL-1	Security Planning Policy and Procedures	6.1 15.1.1	---
3.2.2	PL-2	System Security Plan	6.1	SP-2.1
3.2.3	PL-3	System Security Plan Update	6.1	SP-2.1
3.2.4	PL-4	Rules of Behavior	7.1.3 8.1.3 15.1.5	---
3.2.5	PL-5	Privacy Impact Assessment	15.1.4	---

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
3.2.6	PL-6	Security-Related Activity Planning	15.3.1	---
3.2.7	--	HUD Policy Title – HUD Inventory	--	CC-3
3.2.8	--	HUD Policy Title – ISSO	--	--
Personnel Security				
4.1.1	PS-1	Personnel Security Policy and Procedures	8.1.1 15.1.1	---
4.1.2	PS-2	Position Categorization	8.1.2	SD-1.2
4.1.3	PS-3	Personnel Screening	8.1.2	SP-4.1
4.1.4	PS-4	Personnel Termination	8.1.3 8.3 11.2.1	SP-4.1
4.1.5	PS-5	Personnel Transfer	8.3.1 8.3.3 11.2.1	SP-4.1
4.1.6	PS-6	Access Agreements	6.1.5 8.1.3	SP-4.1
4.1.7	PS-7	Third-Party Personnel Security	6.2.1 6.2.3 8.1.1 8.1.2 8.1.3 8.2.1 8.2.2 11.2.1	SP-4.1
4.1.8	PS-8	Personnel Sanctions	8.2.3 11.2.1	---
Risk Assessment				
3.1.1	RA-1	Risk Assessment Policy and Procedures	4.1 15.1.1	---
3.1.2	RA-2	Security Categorization	7.2.1	SP-1 AC-1.1 AC-1.2
3.1.3	RA-3	Risk Assessment	4.0 4.1 4.2 6.2.1 10.10.2 10.10.5 12.5.1 12.6.1 14.1.1 14.1.2	SP-1
3.1.4	RA-4	Risk Assessment Update	4.1	SP-1
3.1.5	RA-5	Vulnerability Scanning	12.6.1	---
3.1.6		HUD Policy Title – E-Authentication Risk Assessment		

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
System and Services Acquisition				
3.3.1	SA-1	System and Services Acquisition Policy and Procedures	12.1 15.1.1	---
3.3.2	SA-2	Allocation of Resources	10.3.1	---
3.3.3	SA-3	Life Cycle Support	---	---
3.3.4	SA-4	Acquisitions	12.1.1	---
3.3.5	SA-5	Information System Documentation	10.7.4	CC-2.1
3.3.6	SA-6	Software Usage Restrictions	15.1.2	SS-3.2 SP-2.1
3.3.7	SA-7	User Installed Software	15.1.2	SS-3.2
3.3.8	SA-8	Security Engineering Principles	12.1	---
3.3.9	SA-9	External Information System Services	6.2.1 6.2.3 10.2.1 10.2.2 10.6.2	---
3.3.10	SA-10	Developer Configuration Management	12.5.1 12.5.2	SS-3.1 CC-3
3.3.11	SA-11	Developer Security Testing	12.5.1 12.5.2	SS-3.1 CC-2.1
System and Communications Protection				
5.4.1	SC-1	System and Communications Protection Policy and Procedures	10.8.1 15.1.1	---
5.4.2	SC-2	Application Partitioning	11.4.5	---
5.4.3	SC-3	Security Function Isolation	11.4.5	---
5.4.4	SC-4	Information Remnants	10.8.1	AC-3.4
5.4.5	SC-5	Denial of Service Protection	10.8.4 13.2.1	---
5.4.6	SC-6	Resource Priority	---	---
5.4.7	SC-7	Boundary Protection	11.4.6	AC-3.2
5.4.8	SC-8	Transmission Integrity	10.6.1 10.8.1 10.9.1	AC-3.2
5.4.9	SC-9	Transmission Confidentiality	10.6.1 10.8.1 10.9.1	---
5.4.10	SC-10	Network Disconnect	11.5.6	AC-3.2
5.4.11	SC-11	Trusted Path	10.9.2	---
5.4.12	SC-12	Cryptographic Key Establishment and Management	12.3.1 12.3.2	---
5.4.13	SC-13	Use of Cryptography	---	---
5.4.14	SC-14	Public Access Protections	10.7.4 10.9.3	---
5.4.15	SC-15	Collaborative Computing	---	---

HUD POLICY NO.	NIST CNTL NO.	CONTROL NAME	ISO/IEC 17799	GAO FISCAM
5.4.16	SC-16	Transmission of Security Parameters	7.2.2 10.8.2 10.9.2	AC-3.2
5.4.17	SC-17	Public Key Infrastructure Certificates	12.3.2	---
5.4.18	SC-18	Mobile Code	10.4.1 10.4.2	---
5.4.19	SC-19	Voice Over Internet Protocol	---	---
5.4.20	SC-20	Secure Name /Address Resolution Service (Authoritative Source)	---	---
5.4.21	SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	---	---
5.4.22	SC-22	Architecture and Provisioning for Name/Address Resolution Service	---	---
5.4.23	SC-23	Session Authenticity	---	---
System and Information Integrity				
4.6.1	SI-1	System and Information Integrity Policy and Procedures	15.1.1	---
4.6.2	SI-2	Flaw Remediation	10.10.5 12.4.1 12.5.1 12.5.2 12.6.1	SS-2.2
4.6.3	SI-3	Malicious Code Protection	10.4.1	---
4.6.4	SI-4	Information System Monitoring Tools and Techniques	10.6.2 10.10.1 10.10.2 10.10.4	---
4.6.5	SI-5	Security Alerts and Advisories	6.1.7 10.4.1	SP-3.4
4.6.6	SI-6	Security Functionality Verification	---	SS-2.2
4.6.7	SI-7	Software and Information Integrity	12.2.1 12.2.2 12.2.4	---
4.6.8	SI-8	Spam Protection	---	---
4.6.9	SI-9	Information Input Restrictions	12.2.1 12.2.2	SD-1
4.6.10	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3 12.2.1 12.2.2	---
4.6.11	SI-11	Error Handling	12.2.1 12.2.2 12.2.3 12.2.4	---
4.6.12	SI-12	Information Output Handling and Retention	10.7.3 12.2.4	---
4.6.13	---	HUD Policy Title – Electronic Signatures	---	---